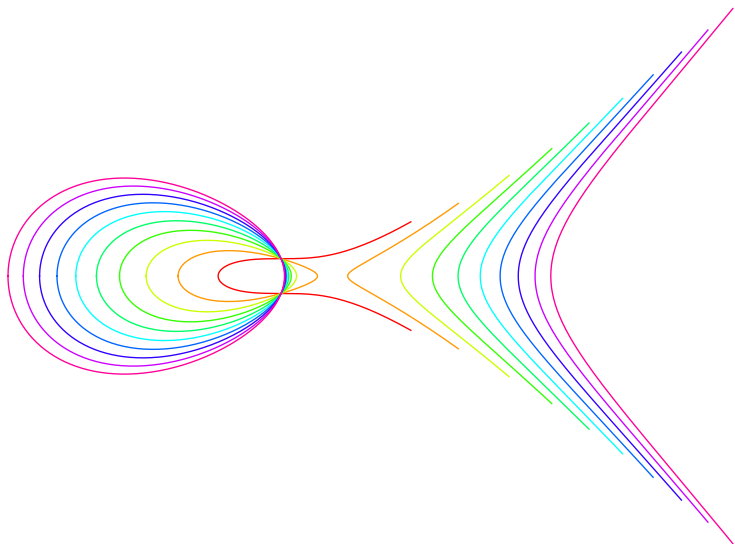


A Whirlwind Tour of Cryptography



Katherine E. Stange, Math 4440/5440 First Day (August 26, 2024)

Ancient Cryptography

א ב ג ד ה ו ז ח ט י כ ל מ נ ס ע פ צ ק ר ש ת
ת ש ר ק צ פ ע ס נ מ ל כ י ט ח ז ו ה ד ג ב א

Atbash Cipher

Jeremiah 25:26 “The king of Sheshach shall drink after them”

(בבל *bb1* → ששך *ššk*)

Ancient Cryptography



Caesar Wheel

image: Subjectiveart, CC BY-SA 4.0 <https://creativecommons.org/licenses/by-sa/4.0>, via Wikimedia Commons

Last 500 years

Vigenère Cipher

| | | | | | | | | | | | | |
|------------|---|---|---|---|---|---|---|---|---|---|---|---|
| KEY | 1 | 3 | 2 | 4 | 1 | 3 | 2 | 4 | 1 | 3 | 2 | 4 |
| PLAINTEXT | A | T | T | A | C | K | A | T | D | A | W | N |
| CIPHERTEXT | B | W | V | E | D | N | C | X | E | D | Y | R |

"impossible of translation" - Scientific American, 1917

Example of a **substitution cipher** (replacing characters)

First World War

| | A | D | F | G | V | X | 3 | 4 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|---|---|
| A | c | o | 8 | x | f | 4 | D | G | X | G |
| D | m | k | 3 | a | z | 9 | X | G | D | G |
| F | n | w | 1 | 0 | j | d | A | A | D | D |
| G | 5 | s | i | y | h | u | D | G | X | G |
| V | p | l | v | b | 6 | r | F | X | D | G |
| X | e | q | 7 | t | 2 | g | F | D | F | A |

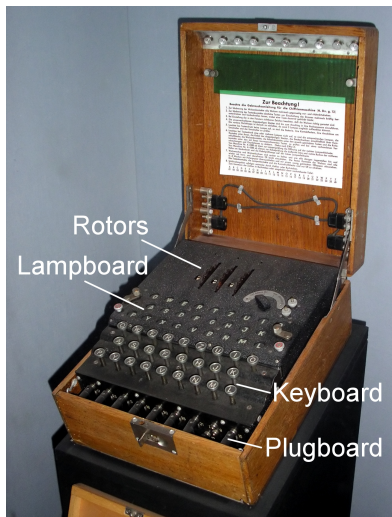
Plaintext: attack at dawn

Step 1: DG XG XG DG AA DD DG XG FX DG FD FA

Ciphertext: GGDGGAXDDXDFDXADFFGGAGXD

Includes an example of a **transposition cipher** (reordering characters)

Second World War



Wartime Enigma Machine

at left: public domain; at right: Bundesarchiv, Bild 101I-769-0229-10A / Borchert, Erich (Eric) / CC-BY-SA 3.0, CC BY-SA 3.0 DE <https://creativecommons.org/licenses/by-sa/3.0/de/deed.en>, via Wikimedia Commons

Second World War



Second World War

Geheime Kommandosache!

Jede einzelne Tageschlüssel ist geheim. Mündl. im Flugzeug verboten!

Nr. 00190

Luftwaffen-Maschinen-Schlüssel Nr. 649

Achtung! Schlüsselmittel dürfen nicht unversehrt in Feindeshand fallen. Bei Gefahr restlos und fröhlich vernichten.

| Tagesnummer 1942 | Wellenlage | | | Ringstellung | 5 teils veränderbare Verbindungen | | | | | | | | | | Kerngruppen | | | | | | | | | | |
|---------------------|------------|-----|-----|--------------|-----------------------------------|----|----|----|----|----------------|---|----|----|----|-------------|----|----|----|----|----|----|-----|-----|-----|-----|
| | | | | | an der Umkehrrolle | | | | | am Statorblech | | | | | | | | | | | | | | | |
| | | | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | | | | | | | | | | | |
| 640 | 31 | I | V | III | 14 09 24 | | | | | | | SZ | GT | DV | KU | FO | MY | EW | JN | IX | LQ | wny | dgy | exb | rzg |
| 640 | 30 | IV | III | II | 05 26 02 | | | | | | | IS | EV | MX | RW | DT | UZ | JQ | AO | CH | NY | kti | acw | zsi | wao |
| 640 | 29 | III | II | I | 12 24 03 | KM | AX | PZ | OO | | | DJ | AT | CV | IO | ER | QS | LW | PZ | PH | BH | ioc | ncn | ovw | wvd |
| 640 | 28 | II | III | V | 06 08 16 | DI | CN | BR | PV | | | CR | PV | AI | DK | OT | MQ | EU | BX | LP | GJ | lrb | cid | ude | rzh |
| 640 | 27 | III | I | IV | 11 03 07 | LT | EQ | HS | UW | | | DY | IN | BV | OR | AM | LO | PP | HT | EX | UW | woj | fbh | vct | uis |
| 640 | 26 | I | IV | V | 17 22 19 | | | | | | | VZ | AL | RT | KO | CO | EI | BJ | DU | FS | HP | xle | gbo | uev | rxm |
| 640 | 25 | IV | III | I | 08 25 12 | | | | | | | OR | PV | AD | IT | FK | HJ | LZ | NS | EQ | CU | ouc | uhq | uew | uit |
| 640 | 24 | V | I | IV | 05 18 14 | | | | | | | TY | AS | ON | KV | JM | DR | HX | GL | CZ | NW | kpl | rw1 | vci | tlq |
| 640 | 23 | IV | II | I | 24 12 04 | | | | | | | QV | FR | AK | EO | DH | CJ | MZ | SX | GN | LT | ebn | rwM | udf | tlo |
| 640 | 22 | II | IV | V | 01 09 21 | IU | AS | DV | GL | | | PJ | ES | IM | RX | LV | AY | OU | BO | WZ | CN | jqc | acx | mwe | wve |
| 640 | 21 | I | V | II | 13 05 19 | PT | OX | EZ | CH | | | RU | HL | PY | OS | OZ | DM | AW | CE | TV | NX | jpw | del | mwf | wvf |
| 640 | 20 | III | IV | V | 24 01 10 | MR | KN | BQ | PW | | | DP | HO | QZ | AU | RY | SV | JL | OX | BE | TW | Jqd | cef | nvo | ysh |
| 640 | 19 | V | III | I | 17 25 20 | | | | | | | OX | PR | PH | WT | DL | CM | AE | TZ | J5 | G1 | idf | fpX | jwg | tlg |
| 640 | 18 | IV | II | V | 15 23 26 | | | | | | | EJ | OY | IV | AQ | KW | FX | MT | PS | LU | BD | lsa | bw | vcj | rxn |
| 640 | 17 | I | IV | II | 21 10 06 | | | | | | | IR | XZ | LS | EM | OV | OT | QX | AP | JP | BU | mae | hzi | sog | ysi |
| 640 | 16 | V | II | III | 08 16 13 | | | | | | | HM | JO | DI | NR | BY | XZ | O5 | PU | FO | CT | tdp | dhb | fkB | uiv |
| 640 | 15 | II | IV | I | 01 03 07 | | | | | | | DZ | HY | MR | OW | LX | AJ | BQ | CO | IP | NT | ldw | hsj | soh | wvg |
| 640 | 14 | IV | I | V | 15 11 05 | AI | BT | MV | HU | | | GM | JR | KS | IY | HZ | PL | AX | BT | CQ | NV | imz | noa | tjv | xtk |
| 640 | 13 | I | III | II | 13 20 03 | PW | EL | DO | KN | | | LY | AG | KM | BR | IQ | JU | HV | SW | ET | CX | zgr | dgz | Gjo | ryg |
| 640 | 12 | V | I | IV | 18 10 07 | | | | | | | MU | BP | CY | RZ | KX | AN | JT | DG | IL | PV | zdy | rkf | tjw | xtl |
| 640 | 11 | II | IV | III | 02 26 15 | RZ | OQ | CP | SX | | | KN | UY | HR | PW | PH | BO | EZ | QT | DX | JV | zea | rjy | soi | wvh |
| 640 | 10 | III | V | III | 23 21 01 | | | | | | | LR | IK | MS | QU | HW | PT | O0 | VX | PZ | EN | lrc | zbx | vbm | rxo |
| 640 | 9 | V | I | III | 16 04 08 | | | | | | | QY | B5 | LN | KT | AP | IU | DU | HO | RV | JZ | edj | eyr | vby | tlh |
| 640 | 8 | IV | II | V | 13 19 25 | | | | | | | PI | NQ | SY | CU | BZ | AH | EL | TX | DO | KP | yiz | dha | ekc | tli |
| 640 | 7 | I | IV | II | 09 03 22 | | | | | | | UX | Iz | HN | BK | OQ | CP | FT | JY | MW | AR | lan | dgB | zsj | wbi |
| 640 | 6 | III | I | V | 11 18 14 | | | | | | | DQ | GU | BW | NP | HK | AZ | CI | PO | JX | YV | lao | cft | zsk | wbj |
| 640 | 5 | V | II | IV | 23 02 25 | | | | | | | MV | CL | OK | OQ | BI | FU | H5 | FX | NW | EY | lju | edr | iyw | waj |
| 640 | 4 | II | IV | I | 04 21 09 | QT | WZ | KV | GM | | | AC | BL | OZ | EK | QV | OP | SU | DH | JM | TX | lsb | zby | vcy | ujb |
| 640 | 3 | V | I | II | 19 11 06 | | | | | | | KR | MP | CN | BP | EH | DZ | IW | AV | OJ | LO | lap | owd | iwu | wak |
| 640 | 2 | IV | V | I | 16 14 02 | BP | NR | DX | CS | | | BN | HU | EO | PY | KQ | CP | O5 | JW | AI | VZ | aqd | bdy | iyf | xtd |
| 640 | 1 | II | I | III | 23 12 10 | | | | | | | DP | BM | NZ | CK | OV | HQ | AP | UY | SW | JO | kg1 | cdf | giq | wuw |

Symmetric Key Cryptography

All the systems discussed so far are **symmetric key cryptosystems**. Such a system consists of:

Symmetric Key Cryptography

All the systems discussed so far are **symmetric key cryptosystems**. Such a system consists of:

1. A **secret key**, i.e. a piece of information that allows for easy encryption and decryption, secretly shared between sender and receiver.

Symmetric Key Cryptography

All the systems discussed so far are **symmetric key cryptosystems**. Such a system consists of:

1. A **secret key**, i.e. a piece of information that allows for easy encryption and decryption, secretly shared between sender and receiver.
2. An **encryption method**, that uses the **secret key** to transform the **plaintext** (the original message, typically in a natural language such as english) into the **ciphertext** (the encrypted message that looks like gobbledygook to the untrained eye).

Symmetric Key Cryptography

All the systems discussed so far are **symmetric key cryptosystems**. Such a system consists of:

1. A **secret key**, i.e. a piece of information that allows for easy encryption and decryption, secretly shared between sender and receiver.
2. An **encryption method**, that uses the **secret key** to transform the **plaintext** (the original message, typically in a natural language such as english) into the **ciphertext** (the encrypted message that looks like gobbledygook to the untrained eye).
3. A **decryption method**, that uses the **secret key** to transform the **ciphertext** into the **plaintext**.

Symmetric Key Cryptography

All the systems discussed so far are **symmetric key cryptosystems**. Such a system consists of:

1. A **secret key**, i.e. a piece of information that allows for easy encryption and decryption, secretly shared between sender and receiver.
2. An **encryption method**, that uses the **secret key** to transform the **plaintext** (the original message, typically in a natural language such as english) into the **ciphertext** (the encrypted message that looks like gobbledygook to the untrained eye).
3. A **decryption method**, that uses the **secret key** to transform the **ciphertext** into the **plaintext**.

Problems: key distribution

Symmetric Key Cryptography

| system | key | encryption | decryption |
|--------|-----|------------|------------|
|--------|-----|------------|------------|

Cesar

Vigenère

ADFGVX

Enigma

Symmetric Key Cryptography

| system | key | encryption | decryption |
|----------|-------|------------------|-------------------|
| Ceasar | shift | shift forward | shift backward |
| Vigenère | | | |
| ADFGVX | | | |
| Enigma | | | |

Symmetric Key Cryptography

| system | key | encryption | decryption |
|----------|--------------------------|--------------------------|---------------------------|
| Ceasar | shift | shift forward | shift backward |
| Vigenère | sequence of shifts | shift forward | shift backward |
| ADFGVX | square & column order | complicated! | complicated backwards! |
| Enigma | machine setup | press key, read light | press key, read light |

Security of a cryptosystem

The **keyspace** is the set of all possible secret keys.

Security of a cryptosystem

The **keyspace** is the set of all possible secret keys.
A **cryptanalyst** tries to break a cryptosystem.

Security of a cryptosystem

The **keyspace** is the set of all possible secret keys.

A **cryptanalyst** tries to break a cryptosystem.

The first, most naïve method is **exhaustive search**: trying all possible keys.

Security of a cryptosystem

The **keyspace** is the set of all possible secret keys.

A **cryptanalyst** tries to break a cryptosystem.

The first, most naïve method is **exhaustive search**: trying all possible keys.

| key | plaintext | key | plaintext |
|-----|-------------|-----|-------------|
| 0 | WFYDAKZLWPL | 13 | JSLQNXMYJCY |
| 1 | XGZEBLAMXQM | 14 | KTMROYNZKDZ |
| 2 | YHAFMBNRYN | 15 | LUNSPZOALEA |
| 3 | ZIBGDNCOZSO | 16 | MVOTQAPBMFB |
| 4 | AJCHEODPATP | 17 | NWPURBQCNGC |
| 5 | BKDIFPEQBUQ | 18 | OXQVSCRDOHD |
| 6 | CLEJGQFRCVR | 19 | PYRWTDSEPIE |
| 7 | DMFKHRGSDWS | 20 | QZSXUETFQJF |
| 8 | ENGLISHTEXT | 21 | RATYVFUGRKG |
| 9 | FOHMJTIUFYU | 22 | SBUZWGVHSLH |
| 10 | GPINKUJVGZV | 23 | TCVAXHWITMI |
| 11 | HQJOLVKWHAW | 24 | UDWBYIXJUNJ |
| 12 | IRKPMWLXIBX | 25 | VEXCZJYKVOK |

What's better than exhaustive search?

A XYDLBAAXR
is LONGFELLOW

One letter stands for another. In this sample, A is used for the three L's, X for the two O's, etc. Single letters, apostrophes, the length and formation of the words are all hints. Each day the code letters are different.

2-28 CRYPTOQUOTE

OWVDOAVSW VC WSA AIB OZA

SY FZOLVWJC AIOA DSHB

XGA ZOAIBZ AIB OZA SY

DSHBD BWAC AIOA OZB

FZOLW. — WSZDOW DPUOZBW

Yesterday's Cryptoquote: ONCE YOU DECIDE TO
TITILLATE INSTEAD OF ILLUMINATE, YOU'RE
ON A SLIPPERY SLOPE. — BILL MOYERS

Source: www.dailyrepublic.com

What's better than exhaustive search?

A XYDLBAAXR
is LONGFELLOW

One letter stands for another. In this sample, A is used for the three L's, X for the two O's, etc. Single letters, apostrophes, the length and formation of the words are all hints. Each day the code letters are different.

2-28 CRYPTOQUOTE

OWVDOAVSW VC WSA AIB OZA

SY FZOLVWJC AIOA DSHB

XGA ZOAIBZ AIB OZA SY

DSHBD BWAC AIOA OZB

FZOLW. — WSZDOW DPUOZBW

Yesterday's Cryptoquote: ONCE YOU DECIDE TO
TITILLATE INSTEAD OF ILLUMINATE, YOU'RE
ON A SLIPPERY SLOPE. — BILL MOYERS

Source: www.dailyrepublic.com

The number of possible keys: 26!

What's better than exhaustive search?

A XYDLBAAXR
is LONGFELLOW

One letter stands for another. In this sample, A is used for the three L's, X for the two O's, etc. Single letters, apostrophes, the length and formation of the words are all hints. Each day the code letters are different.

2-28 CRYPTOQUOTE

OWVDOAVSW VC WSA AIB OZA

SY FZOLVWJC AIOA DSHB

XGA ZOAIBZ AIB OZA SY

DSHBD BWAC AIOA OZB

FZOLW. — WSZDOW DPUOZBW

Yesterday's Cryptoquote: ONCE YOU DECIDE TO
TITILLATE INSTEAD OF ILLUMINATE, YOU'RE
ON A SLIPPERY SLOPE. — BILL MOYERS

Source: www.dailyrepublic.com

The number of possible keys: 26!

$> 400,000,000,000,000,000,000,000 = 4 \times 10^{26}$.

The enigma keyspace

Geheime Kommandosache!

Jede einzelne Tagesstiftel ist geheim. Mithin: im Flugzeug verboten!

Nr. 00190

Luftwaffen-Maschinen-Schlüssel Nr. 649

Achtung! Schlüsselmittel dürfen nicht unversehrt in Feindeshand fallen. Bei Gefahr restlos und fröhlichzeitig vernichten.

| Tagesstiftel Nr. | Wellenlage | Ringstellung | Stellenverbindungen | | | | | | | | | | Benutzgruppen | | | | | | | | | | | |
|---------------------|------------|--------------|---------------------|----|----|----|----|-----------------|----|----|----|----|---------------|----|----|----|----|----|----|----|-----|-----|-----|-----|
| | | | an der Buchstabe | | | | | am Stecherbrett | | | | | | | | | | | | | | | | |
| | | | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | | | | | | | | | | | | |
| 040 31 | I | V | III | 14 | 06 | 24 | | | | | SZ | GT | DV | KU | FO | MY | EW | JH | IX | LQ | wny | dgy | exb | rfg |
| 040 30 | IV | III | II | 05 | 26 | 02 | | | | | IS | EV | MX | RW | DT | UZ | JQ | AO | CH | NY | kti | acw | zsi | wzo |
| 040 29 | III | II | I | 12 | 24 | 03 | KM | AX | PZ | OO | DJ | AT | CV | IO | ER | QS | LW | PZ | FN | BH | ioc | acn | ovw | vwd |
| 040 28 | II | III | V | 06 | 08 | 16 | DI | CH | BR | PV | CR | PV | AI | DK | OT | MQ | EU | BX | LP | GJ | lrb | cid | ude | rzh |
| 040 27 | III | I | IV | 11 | 03 | 07 | LT | EQ | HS | UW | DY | IN | BV | QR | AM | LO | FP | HT | EX | UW | woj | fbh | vct | uis |
| 040 26 | I | IV | V | 17 | 22 | 19 | | | | | VZ | AL | RT | KO | CO | EI | BJ | DU | F5 | HP | xle | gbo | uev | rxm |
| 040 25 | IV | III | I | 08 | 25 | 12 | | | | | OR | PV | AD | IT | PK | HJ | LZ | NS | EQ | CW | ouc | uhq | uew | uit |
| 040 24 | V | I | IV | 05 | 18 | 14 | | | | | TY | AS | OW | KV | JM | DR | HL | GX | CZ | NU | kpl | rwl | vci | tlq |
| 040 23 | IV | II | I | 24 | 12 | 04 | | | | | QV | FR | AK | EO | DH | CJ | KE | SX | ON | LT | ebn | rwm | udf | tlo |
| 040 22 | II | IV | V | 01 | 09 | 21 | IU | AS | DV | GL | PJ | ES | IM | RX | LV | AY | OU | BO | WZ | CN | jqc | acx | mwe | wvc |
| 040 21 | I | V | II | 13 | 05 | 19 | PT | OX | EZ | CH | RU | HL | PY | OS | GZ | DM | AW | CE | TV | NX | jpw | del | mwf | wvf |
| 040 20 | III | IV | V | 24 | 01 | 10 | MR | KN | BQ | PW | DF | HO | QE | AU | RY | SV | JL | OX | BE | TW | jgd | cef | nvo | ysh |
| 040 19 | V | III | I | 17 | 25 | 20 | | | | | OX | FR | PH | WY | DL | CM | AE | TZ | J5 | G1 | idf | fpz | jwg | tig |
| 040 18 | IV | II | V | 15 | 23 | 26 | | | | | EJ | OY | IV | AQ | KW | FX | MT | F5 | LU | BD | isa | gbw | vcj | rxn |
| 040 17 | I | IV | II | 21 | 10 | 06 | | | | | IR | KZ | LS | EM | OY | QX | AP | JF | BU | | mae | hti | soE | ysi |
| 040 16 | V | II | III | 08 | 16 | 13 | | | | | HM | JO | DI | NR | BY | XZ | 05 | PU | FQ | CT | tdp | dhb | fkf | uiv |
| 040 15 | II | IV | I | 01 | 03 | 07 | | | | | DS | HY | NR | OW | LX | AJ | BQ | CO | IP | MT | ldw | htj | soh | wvg |
| 040 14 | IV | I | V | 15 | 11 | 05 | AI | BT | MV | HU | GM | JR | KS | IY | HZ | PL | AX | BT | CQ | NV | imz | noa | tjv | xtk |
| 040 13 | I | III | II | 13 | 20 | 03 | PW | EL | DO | KN | LY | AG | KM | BR | IQ | JU | HV | SW | ET | CX | zgr | dgz | gjo | ryg |
| 040 12 | V | I | IV | 18 | 10 | 07 | | | | | MU | BP | CY | RZ | KX | AN | JT | DG | IL | PW | zdy | rkf | tjw | xtl |
| 040 11 | II | IV | III | 02 | 26 | 15 | RZ | OQ | CP | SX | KN | UY | HR | PW | PM | BO | EZ | QT | DJ | VJ | zea | rjy | soi | whv |
| 040 10 | III | V | I | 23 | 21 | 01 | | | | | LR | IK | MS | QU | HW | PT | 00 | VX | FZ | EN | lrc | zbx | vbm | rxo |
| 040 9 | V | I | III | 16 | 04 | 08 | | | | | QT | BS | LN | KT | AP | IU | DW | HO | RV | JZ | edj | eyr | vby | tih |
| 040 8 | IV | II | V | 13 | 19 | 25 | | | | | PI | NQ | SY | CU | BE | AH | EL | TX | DO | KP | yiz | dha | ekc | tli |
| 040 7 | I | IV | II | 09 | 03 | 22 | | | | | UX | IE | HN | BK | OQ | CP | FT | JY | HW | AR | lan | dgb | zsj | wbi |
| 040 6 | III | I | V | 11 | 18 | 14 | | | | | DQ | QU | BW | NP | HK | AZ | CI | PO | JX | VY | lau | ctf | zsk | wbj |
| 040 5 | V | II | IV | 23 | 02 | 25 | IL | AP | EU | HO | MV | GL | OK | OQ | BI | FU | H5 | PX | NW | EY | lso | edr | iyw | waj |
| 040 4 | II | IV | I | 04 | 21 | 09 | QT | WZ | KV | GM | AC | BL | OZ | EK | QV | OP | SU | DH | JM | TX | lsp | zwd | iwu | wak |
| 040 3 | V | I | II | 19 | 11 | 06 | BP | NR | DX | CS | KR | MP | CN | BP | EH | DZ | IW | AV | GJ | LO | aqd | bdy | iyf | xtd |
| 040 2 | IV | V | I | 16 | 14 | 02 | | | | | BN | HU | EO | PY | KQ | CP | OS | JW | AI | VZ | agd | bdy | iyf | xtd |
| 040 1 | II | I | III | 23 | 12 | 10 | | | | | DP | BM | NZ | CK | OY | HQ | AP | UY | SW | J0 | kgl | edf | giq | wuv |

The enigma keyspace

Geheime Kommandosache! Jede einzelne Tagesstiftel ist geheim. Minder im Flugzeug verboten! Nr. 00190

Luftwaffen-Maschinen-Schlüssel Nr. 649

Achtung! Schlüsselmittel dürfen nicht unversehrt in Feindeshand fallen. Bei Gefahr restlos und fröhlich vernichten.

| Tagesstiftel Nr. 1-31 | Wellenlage | Ringstellung | Stellenverbindungen | | | | | | | | | | Benutzgruppen | | | | | | |
|--------------------------|------------|--------------|---------------------|-----|--|----|----|-----------------|----|----|----|----|---------------|----|----|-----|-----|-----|-----|
| | | | an der Buchstabe | | | | | am Stecherblech | | | | | | | | | | | |
| | | | | | | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | | |
| 040 | | 4 06 24 | | | | SZ | GT | DV | KU | FO | MY | EW | JH | IX | LQ | wny | dgy | exb | rfg |
| 040 | | 05 26 02 | | | | IS | EV | MX | RW | DT | UZ | JQ | AO | CH | NY | kti | acw | zsi | wzo |
| 040 | | 12 24 03 | | | | KM | AX | PZ | OO | DJ | AT | CV | IO | ER | QS | LW | PZ | FN | BH |
| 040 | | 06 08 16 | | | | DI | CH | BR | PV | CR | PV | AI | DK | OT | MQ | EU | BX | LP | GJ |
| 040 | 28 | III V | | | | LT | EQ | HS | UW | DY | IN | BV | QR | AM | LO | FP | HT | EX | UW |
| 040 | 27 | III I | IV | | | | | | | VZ | AL | RT | KO | CO | EI | BJ | DU | F5 | HP |
| 040 | 26 | I | IV | V | | | | | | OR | PV | AD | IT | PK | HJ | LZ | NS | EQ | CW |
| 040 | 25 | IV | III | I | | | | | | TY | AS | OW | KV | JM | DR | HX | GL | CZ | NU |
| 040 | 24 | V | I | IV | | | | | | QV | FR | AK | EO | DH | CJ | KE | SX | ON | LT |
| 040 | 23 | IV | II | I | | | | | | PJ | ES | IM | RX | LV | AY | OU | BO | WZ | CN |
| 040 | 22 | II | IV | V | | | | | | IU | AS | DV | GL | | | | | | |
| 040 | 21 | I | V | II | | | | | | RU | HL | PY | OS | GZ | DM | AW | CE | TV | NX |
| 040 | 20 | III | IV | V | | | | | | PT | OX | EZ | CH | | | | | | |
| 040 | 19 | V | III | I | | | | | | MR | KN | BQ | PW | | | | | | |
| 040 | 18 | IV | II | V | | | | | | OX | FR | PH | WY | DL | CM | AE | TZ | J5 | G1 |
| 040 | 17 | I | IV | II | | | | | | EJ | OY | IV | AQ | KW | FX | MT | F5 | LU | BD |
| 040 | 16 | V | II | III | | | | | | IR | KZ | LS | EM | OY | OY | QX | AP | JP | BU |
| 040 | 15 | II | IV | I | | | | | | HM | JO | DI | NR | BY | XZ | OS | PU | FQ | CT |
| 040 | 14 | IV | I | V | | | | | | DS | HY | NR | OW | LX | AJ | BQ | CO | IP | MT |
| 040 | 13 | I | III | II | | | | | | AI | BT | MV | HU | | | | | | |
| 040 | 12 | V | I | IV | | | | | | OM | JR | KS | IY | HZ | PL | AX | BT | CO | NV |
| 040 | 11 | II | IV | III | | | | | | LY | AG | KM | BR | IQ | JU | HV | SW | ET | CX |
| 040 | 10 | III | V | IV | | | | | | MU | BP | CY | RZ | KX | AN | JT | DG | IL | PW |
| 040 | 9 | V | I | III | | | | | | RZ | OQ | CP | SX | | | | | | |
| 040 | 8 | IV | II | V | | | | | | KN | UY | HR | PW | PM | BO | EZ | QT | DJ | VJ |
| 040 | 7 | I | IV | II | | | | | | LR | IK | MS | QU | HV | PT | OO | VX | FZ | EN |
| 040 | 6 | III | I | V | | | | | | QY | V | LN | KT | AP | IU | DW | HO | RV | JZ |
| 040 | 5 | II | IV | I | | | | | | PI | NQ | SY | CU | BE | AH | EL | TX | DO | KP |
| 040 | 4 | V | I | III | | | | | | UX | IZ | HN | BK | OQ | CP | FT | JY | HW | AR |
| 040 | 3 | IV | V | I | | | | | | DQ | OU | BW | NP | HK | AZ | CI | PO | JX | VY |
| 040 | 2 | II | I | III | | | | | | MV | CL | OK | OQ | BI | FU | H5 | PX | NW | ET |
| 040 | 1 | I | III | II | | | | | | IL | AP | EU | HO | | | | | | |
| 040 | | | | | | | | | | QT | WZ | KV | GM | | | | | | |
| 040 | | | | | | | | | | AC | BL | OZ | EK | QV | OP | SU | DH | JM | TX |
| 040 | | | | | | | | | | KR | MP | CN | BP | EH | DZ | IW | AV | GJ | LO |
| 040 | | | | | | | | | | BN | HU | EO | PY | KQ | CP | OS | JW | AI | VZ |
| 040 | | | | | | | | | | DP | BM | NZ | CK | OY | HQ | AP | UY | SW | JQ |

5 · 4 · 3

The enigma keypspace

Geheime Kommandosache! Jede einzelne Tagesstiftung ist geheim. Minder im Flugzeug verboten! Nr. 00190

Luftwaffen-Maschinen-Schlüssel Nr. 649

Achtung! Schlüsselmittel dürfen nicht unversehrt in Feindeshand fallen. Bei Gefahr restlos und frühzeitig vernichten.

| Tagesstiftung | Wolvenlage | | Stellenverbindungen | | | | | | | | | | Nenngruppen | | | | |
|---------------|--------------|--------------|---------------------|-----|----------|----|----|-----------------|----|----|----|----|-------------|----|----|---------|---------|
| | Ringstellung | Ringstellung | an der Buchstabe | | | | | am Stecherblech | | | | | 1 | 2 | | | |
| | | | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | | | | | |
| 040 | 4 | 06 24 | | | | SZ | GT | DV | KU | FO | MY | EW | JH | IX | LQ | wny dgy | exb rrg |
| 040 | 15 | 05 26 02 | | | | IS | EV | MX | RW | DT | UZ | JQ | AO | CH | NY | ktl acw | zsl wzo |
| 040 | 12 | 24 03 | KM | AX | PZ | 00 | DJ | AT | CV | IO | ER | QS | LW | PZ | FN | ioc acn | ovw rzd |
| 040 | 28 | 06 08 16 | DI | CH | BR | PV | CR | PV | AI | DK | OT | MQ | EU | BX | LP | lrb cid | ude rsh |
| 040 | 27 | 11 03 07 | LT | EQ | HS | UW | DY | IN | BV | QR | AM | LO | PP | HT | EX | woj fbh | vct uis |
| 040 | 26 | | | | | | VZ | AL | RT | KO | CO | EI | BJ | DU | P5 | xle gbo | uev rxm |
| 040 | 25 | | | | | | OR | PV | AD | IT | PK | HJ | LZ | NS | EQ | ouc uhq | uew uit |
| 040 | 24 | V | I | | | | TY | AS | OW | KV | JM | DR | HX | GL | CZ | kpl rwi | vci tlg |
| 040 | 23 | IV | II | | | | QV | FR | AK | EO | DH | CJ | KE | SX | ON | ebn rwm | udf tlo |
| 040 | 22 | II | IV | V | 01 09 21 | | IU | AS | DV | GL | PJ | ES | IM | RX | LV | jqc acx | mwe wvc |
| 040 | 21 | I | V | II | 13 05 19 | | PT | OX | EZ | CH | RU | HL | PY | OS | GZ | jpw del | mwf wvf |
| 040 | 20 | III | IV | V | 24 01 10 | | MR | KN | BQ | PW | DF | HO | QE | AU | RY | jqd cef | nvo ysh |
| 040 | 19 | V | III | I | 17 25 20 | | | | | | OX | FR | PH | WY | DL | idf fpx | jwg tlg |
| 040 | 18 | IV | II | V | 15 23 26 | | | | | | EJ | OY | IV | AQ | KW | isa gbw | vcj rxn |
| 040 | 17 | I | IV | II | 21 10 06 | | | | | | IR | KZ | LS | EM | OY | mae hti | soE ysi |
| 040 | 16 | V | II | III | 08 16 13 | | | | | | HM | JO | DI | NR | BY | tdp dbh | fkv uiv |
| 040 | 15 | II | IV | I | 01 03 07 | | | | | | DS | HY | NR | OW | LX | ldw hjz | soh wvg |
| 040 | 14 | IV | I | V | 15 11 05 | AI | BT | MV | HU | | GM | JR | KS | IY | HZ | cmv | imz noa |
| 040 | 13 | I | III | II | 13 20 03 | | | | | | LY | AG | KM | BR | IQ | zgr dgs | gjo ryg |
| 040 | 12 | V | I | | 18 10 07 | | | | | | MU | BP | CY | RZ | KX | zdy rxf | tjw xtl |
| 040 | 11 | II | IV | III | 02 26 15 | RZ | OQ | CP | SX | | KN | UY | HR | PW | PM | sea rjy | soi vwh |
| 040 | 10 | III | V | IV | 23 21 01 | | | | | | LR | IK | MS | QU | HW | lrc zbx | vbm rxo |
| 040 | 9 | V | I | III | 16 04 08 | | | | | | QY | BS | LN | KT | AP | edj eyr | vby tih |
| 040 | 8 | IV | II | V | 13 19 25 | | | | | | PI | NQ | SY | CU | BE | yiz dha | ekc tli |
| 040 | 7 | I | IV | II | 09 03 22 | | | | | | UX | IZ | HN | BK | OQ | lan dgb | zsj wbi |
| 040 | 6 | III | I | V | 11 18 14 | | | | | | DQ | QU | BW | NP | HK | lao cft | zsk wbj |
| 040 | 5 | V | II | IV | 23 02 25 | IL | AP | EU | HO | | MV | GL | OK | OQ | BI | lju cdr | iyv waj |
| 040 | 4 | II | IV | I | 04 21 09 | | | | | | QT | WZ | KV | GM | | lsp zwd | iwu wak |
| 040 | 3 | V | I | II | 19 11 06 | | | | | | BP | NR | DX | CS | | 1ab oby | iyf xtd |
| 040 | 2 | IV | V | I | 16 14 02 | | | | | | BN | HU | EO | PY | KQ | agd bdy | iyf xtd |
| 040 | 1 | II | I | III | 23 12 10 | | | | | | DP | BM | NZ | CK | OY | kgl cdf | giq wuv |

$$5 \cdot 4 \cdot 3 \cdot 26^3$$

The enigma keypspace

Geheime Kommandosache! Jede einzelne Tagesstiftung ist geheim. Minder im Flugzeug verboten! Nr. 00190

Luftwaffen-Maschinen-Schlüssel Nr. 649

Achtung! Schlüsselmittel dürfen nicht unversehrt in Feindeshand fallen. Bei Gefahr restlos und fröhzeitig vernichten.

| Tagesstiftung | Wellenlage | Ringstellung | Stellenverbindungen | | | | | | | | | | Nenngruppen | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---------------|------------|--------------|---------------------|-----|----|----|----|-----------------|---|---|----|----|-------------|----|----|----|----|----|----|----|-----|-----|-----|-----|-----|-----|-----|-----|----|----|----|----|----|----|--|--|--|--|--|--|--|--|--|--|
| | | | an der Buchstabe | | | | | am Stecherblech | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 040 | | 4 06 24 | | | | | | | | | SZ | GT | DV | KU | FO | MY | EW | JH | IX | LQ | wny | dgy | exb | rfg | | | | | | | | | | | | | | | | | | | | |
| 040 | | 05 26 02 | | | | | | | | | IS | EV | MX | RW | DT | UZ | JQ | AO | CH | NY | kti | acw | zsi | wzo | | | | | | | | | | | | | | | | | | | | |
| 040 | | 12 24 03 | | | | | | | | | KM | AX | PZ | OO | DJ | AT | CV | IO | ER | QS | LW | PZ | FN | BH | ioc | acn | ovw | vvd | | | | | | | | | | | | | | | | |
| 040 | | 06 08 16 | | | | | | | | | DI | CH | BR | PV | CR | PV | AI | DK | OT | MQ | EU | BX | LP | GJ | lrb | cid | ude | rzh | | | | | | | | | | | | | | | | |
| 040 | 28 | III V | IV | 06 | 08 | 16 | | | | | LT | EQ | HS | UW | DY | IN | BV | QR | AM | LO | PP | HT | EX | UW | woj | fbh | vct | uis | | | | | | | | | | | | | | | | |
| 040 | 27 | III I | IV | 11 | 03 | 07 | | | | | | | | | VZ | AL | RT | KO | CO | EI | BJ | DU | P5 | HP | xle | gbo | uev | rxm | | | | | | | | | | | | | | | | |
| 040 | 26 | I | IV | | | | | | | | | | | | OR | PV | AD | IT | PK | HJ | LZ | MS | EQ | CW | ouc | uhq | uew | uit | | | | | | | | | | | | | | | | |
| 040 | 25 | IV | III | | | | | | | | | | | | | | | | | | | | | | kpl | rwl | vci | tlq | | | | | | | | | | | | | | | | |
| 040 | 24 | V | I | | | | | | | | | | | | | | | | | | | | | | ebn | rwm | udf | tlo | | | | | | | | | | | | | | | | |
| 040 | 23 | IV | II | | | | | | | | | | | | | | | | | | | | | | jqc | acx | mwe | wvc | | | | | | | | | | | | | | | | |
| 040 | 22 | II | IV | V | 01 | 09 | 21 | | | | | | | | | | | | | | | | | | jpw | del | mwf | wvf | | | | | | | | | | | | | | | | |
| 040 | 21 | I | V | II | 13 | 05 | 19 | | | | | | | | | | | | | | | | | | qjd | cef | nvo | ysh | | | | | | | | | | | | | | | | |
| 040 | 20 | III | IV | V | 24 | 02 | | | | | | | | | | | | | | | | | | | idf | fpz | jwg | tfg | | | | | | | | | | | | | | | | |
| 040 | 19 | V | III | I | 17 | 22 | | | | | | | | | | | | | | | | | | | isa | gbw | vcj | rxn | | | | | | | | | | | | | | | | |
| 040 | 18 | IV | II | V | 15 | 23 | | | | | | | | | | | | | | | | | | | mae | hti | soE | ysi | | | | | | | | | | | | | | | | |
| 040 | 17 | I | IV | II | 21 | 10 | 06 | | | | | | | | | | | | | | | | | | tdp | dhb | fkv | uiv | | | | | | | | | | | | | | | | |
| 040 | 16 | V | II | III | 08 | 16 | 13 | | | | | | | | | | | | | | | | | | ldw | hvj | soh | wvg | | | | | | | | | | | | | | | | |
| 040 | 15 | II | IV | I | 01 | 03 | 07 | | | | | | | | | | | | | | | | | | imz | noa | tjv | xtk | | | | | | | | | | | | | | | | |
| 040 | 14 | IV | I | V | 15 | 11 | 05 | | | | | | | | | | | | | | | | | | zgr | dgz | gjo | ryg | | | | | | | | | | | | | | | | |
| 040 | 13 | I | III | II | 13 | 20 | 03 | | | | | | | | | | | | | | | | | | zdy | rkf | tjw | xtl | | | | | | | | | | | | | | | | |
| 040 | 12 | V | I | IV | 18 | 10 | 07 | | | | | | | | | | | | | | | | | | zea | rjy | soi | whv | | | | | | | | | | | | | | | | |
| 040 | 11 | II | IV | III | 02 | 26 | 15 | | | | | | | | | | | | | | | | | | lrc | zbx | vbm | rxo | | | | | | | | | | | | | | | | |
| 040 | 10 | III | V | IV | 23 | 21 | 01 | | | | | | | | | | | | | | | | | | edj | eyr | vby | tih | | | | | | | | | | | | | | | | |
| 040 | 9 | V | I | III | 16 | 04 | 08 | | | | | | | | | | | | | | | | | | yiz | dha | ekc | tli | | | | | | | | | | | | | | | | |
| 040 | 8 | IV | II | V | 13 | 19 | 25 | | | | | | | | | | | | | | | | | | lan | dgb | zsj | wbi | | | | | | | | | | | | | | | | |
| 040 | 7 | I | IV | II | 09 | 03 | 22 | | | | | | | | | | | | | | | | | | lao | ctf | zsk | wbj | | | | | | | | | | | | | | | | |
| 040 | 6 | III | I | V | 11 | 18 | 14 | | | | | | | | | | | | | | | | | | lju | edr | iye | waj | | | | | | | | | | | | | | | | |
| 040 | 5 | V | II | IV | 23 | 02 | 25 | | | | | | | | | | | | | | | | | | lsp | zwy | vcy | ujb | | | | | | | | | | | | | | | | |
| 040 | 4 | II | IV | I | 04 | 21 | 09 | | | | | | | | | | | | | | | | | | lzb | owd | iwu | wak | | | | | | | | | | | | | | | | |
| 040 | 3 | V | I | II | 19 | 11 | 06 | | | | | | | | | | | | | | | | | | agd | bdy | iyf | xtd | | | | | | | | | | | | | | | | |
| 040 | 2 | IV | V | I | 16 | 14 | 02 | | | | | | | | | | | | | | | | | | kgl | edf | giq | wuv | | | | | | | | | | | | | | | | |
| 040 | 1 | II | I | III | 23 | 12 | 10 | | | | | | | | | | | | | | | | | | DP | BM | NZ | CK | QV | HQ | AP | UY | SW | JZ | | | | | | | | | | |

rotors

ring

reflector

$$5 \cdot 4 \cdot 3 \cdot 26^3 \cdot 24! / (12! 2^{12})$$

The enigma keystate

Geheime Kommandosache! Jede einzelne Tagesstiftung ist geheim. Minder im Flugzeug verboten! Nr. 00190

Luftwaffen-Maschinen-Schlüssel Nr. 649

Achtung! Schlüsselmittel dürfen nicht unversehrt in Feindeshand fallen. Bei Gefahr zerstört und frühzeitig vernichten.

| Tagesstiftung | Wellenlage | Ringstellung | Städteverbindungen | | | | | | | | | | Benutzgruppen | | | | | | |
|---------------|------------|--------------|----------------------|----|----|----|----|-----------------|----|----|----|----|---------------|----|----|-----|-----|-----|-----|
| | | | an der Blockschleife | | | | | am Stecherblock | | | | | | | | | | | |
| 040 | | 4 06 24 | | | | SZ | GT | DV | KU | FO | MY | EW | JH | IX | LQ | wny | dgy | exb | rfg |
| 040 | | 05 26 02 | | | | IS | EV | MX | RW | DT | UZ | JQ | AO | CH | NY | ktl | acw | zsl | wzo |
| 040 | | 12 24 03 | KM | AX | PZ | 00 | DJ | AT | CV | IO | ER | QS | LW | PZ | FN | lbc | acn | ovw | vvd |
| 040 | | 06 08 16 | DI | CH | BR | PV | CR | PV | AI | DK | OT | MQ | EU | BX | LP | lrb | cid | ude | rzh |
| 040 | 28 | III V | LT | EQ | HS | UW | DY | IN | BV | QR | AM | LO | PP | HT | EX | woj | fbh | vct | uis |
| 040 | 27 | III I | IV | 11 | 03 | 07 | DY | IN | BV | QR | AM | LO | PP | HT | EX | xle | gbo | uev | rxm |
| 040 | 26 | I IV | | | | | VZ | AL | RT | KO | CO | EI | BJ | DU | F5 | ouc | uhq | uew | uit |
| 040 | 25 | IV III | | | | | OR | PV | AD | IT | PK | HJ | LZ | MS | EQ | ouc | uhq | uew | uit |
| 040 | 24 | V I | | | | | TY | AS | OW | KV | JM | DR | HX | GL | CZ | kpl | rw1 | vci | tlq |
| 040 | 23 | IV II | | | | | QV | FR | AK | EO | DH | CJ | KZ | SX | ON | ebn | rw1 | udf | tlc |
| 040 | 22 | II IV | V | 01 | 09 | 21 | IU | AS | DV | GL | | | | | | jqc | acx | mwe | wvc |
| 040 | 21 | I V | II | 13 | 05 | 19 | ET | OX | KZ | CH | | | | | | jpw | del | mwf | wvf |
| 040 | 20 | III IV | V | 24 | 00 | | | | | | QE | AU | RY | SV | JL | ox | ce | ef | ysh |
| 040 | 19 | V III | I | 17 | 00 | | | | | | PH | WY | DL | CM | AE | TZ | J5 | G1 | idf |
| 040 | 18 | IV II | V | 15 | 02 | | | | | | IV | AQ | KW | FX | MT | F5 | LU | BD | isa |
| 040 | 17 | I IV | II | 21 | 10 | 00 | | | | | FR | EL | LS | EM | OV | OY | QX | AP | JF |
| 040 | 16 | V II | III | 08 | 16 | 13 | HM | JO | DI | NR | BY | XZ | 05 | PU | FQ | CT | | | |
| 040 | 15 | II IV | I | 01 | 03 | 07 | DS | HY | NR | OW | LX | AJ | BQ | CO | IP | NT | ldw | h2j | soh |
| 040 | 14 | IV I | V | 15 | 11 | 05 | AI | BT | MV | HU | GM | | | | | | imz | noa | tjv |
| 040 | 13 | I III | II | 13 | 20 | 03 | PW | EL | DO | KN | LY | | | | | | zgr | d2z | gjo |
| 040 | 12 | V I | | 18 | 10 | 07 | MU | | | | | | | | | | zdy | rkf | tjw |
| 040 | 11 | II IV | III | 02 | 26 | 15 | RZ | OQ | CP | SX | KN | | | | | | zsa | rjy | soi |
| 040 | 10 | III V | IV | 23 | 21 | 01 | | | | | LR | IK | MS | QU | HV | PT | 00 | VX | PZ |
| 040 | 9 | V I | III | 16 | 04 | 08 | | | | | QT | B5 | LN | KT | AP | IU | DW | HO | RV |
| 040 | 8 | IV II | V | 13 | 19 | 25 | | | | | PI | NQ | SY | GU | BZ | AH | EL | TX | DO |
| 040 | 7 | I IV | II | 09 | 03 | 22 | | | | | UX | IZ | HN | BK | OQ | CP | FT | JY | HW |
| 040 | 6 | III I | V | 11 | 18 | 14 | | | | | DQ | QU | BW | NP | HK | AZ | CI | PO | JX |
| 040 | 5 | V II | IV | 23 | 02 | 25 | MV | GL | OK | OQ | BI | FU | H5 | PX | HN | EY | | | |
| 040 | 4 | II IV | I | 04 | 21 | 09 | QT | VZ | KV | GM | AC | BL | OZ | EK | QV | OP | SU | DH | JM |
| 040 | 3 | V I | II | 19 | 11 | 06 | BP | NR | DX | CS | KR | MP | CN | BP | EH | DZ | IW | AV | GJ |
| 040 | 2 | IV V | I | 16 | 14 | 02 | | | | | BN | HU | EO | PY | KQ | CP | O5 | JW | AI |
| 040 | 1 | III I | III | 23 | 12 | 10 | | | | | DP | BM | NZ | CK | QV | HQ | AP | UY | 5W |

rotors

ring

reflector

plugboard

positions

$$5 \cdot 4 \cdot 3 \cdot 26^3 \cdot 24! / (12! 2^{12}) \cdot 26! / (10! 6! 2^{10}) \cdot 26^3$$

The enigma keystate

Geheime Kommandosache! Jede einzelne Tagesstiftel ist geheim. Minder im Flugzeug verboten! Nr. 00190

Luftwaffen-Maschinen-Schlüssel Nr. 649

Achtung! Schlüsselmittel dürfen nicht unversehrt in Feindeshand fallen. Bei Gefahr restlos und fröhzeitig vernichten.

| Tagesstiftel Mo | Wellenlage | Ringstellung | Städteverbindungen | | | | | | | | | | Benutzgruppen | | | | |
|--------------------|------------|--------------|----------------------|----|----|----|----|-----------------|----|----|----|----|---------------|----|----|---------|---------|
| | | | an der Blockschleife | | | | | am Stecherblock | | | | | | | | | |
| 040 | | 4 06 24 | | | | SZ | GT | DV | KU | FO | MY | EW | JH | IX | LQ | wny dgy | exb rrg |
| 040 | | 05 26 02 | | | | IS | EV | MX | RW | DT | UZ | JQ | AO | CH | NY | ktl acw | zsl wzo |
| 040 | | 12 24 03 | KM | AX | PZ | 00 | DJ | AT | CV | IO | ER | QS | LW | PZ | FN | lbc acn | ovw vvd |
| 040 | 28 | II III V | DI | CH | BR | PV | CR | PV | AI | DK | OT | MQ | EU | BX | LP | lrb cid | ude rzh |
| 040 | 27 | III I IV | LT | EQ | HS | UW | DY | IN | BV | QR | AM | LO | PP | HT | EX | woj fbb | vct uis |
| 040 | 26 | I IV | | | | | VZ | AL | RT | KO | CO | EI | BJ | DU | FS | xle gbo | uev rxm |
| 040 | 25 | IV III | | | | | OR | PV | AD | IT | PK | HJ | LZ | MS | EQ | ouc uhq | uew uit |
| 040 | 24 | V I | | | | | TY | AS | OW | KV | JM | DR | HX | GL | CZ | kpl rwl | vci tlg |
| 040 | 23 | IV II | | | | | QV | FR | AK | EO | DH | CJ | KZ | SX | ON | ebn rwm | udf tlo |
| 040 | 22 | II IV V | IU | AS | DV | GL | PJ | ES | IM | RX | LV | AY | OU | BO | WZ | jqc acx | mwe wvc |
| 040 | 21 | I V II | ET | OX | KZ | CH | RU | HL | PY | OS | GZ | DM | AW | CE | TV | jpw del | mwf wvf |
| 040 | 20 | III IV V | | | | | QE | AU | RY | SV | JL | OX | BE | TW | | jgd cef | nvo ysh |
| 040 | 19 | V III I | | | | | PH | WY | DL | CM | AE | TZ | J5 | G1 | | idf fpx | jwg tlg |
| 040 | 18 | IV II V | | | | | IV | AQ | KW | FX | MT | FS | LU | BD | | isa gbw | vcj rxn |
| 040 | 17 | I IV II | | | | | FR | EL | LS | EM | OY | OY | QX | AP | JP | mae hti | soE ysi |
| 040 | 16 | V II III | HM | JO | DI | NR | BV | XZ | OS | PU | FQ | CT | | | | tdp dhh | fkb uiv |
| 040 | 15 | II IV I | DS | HY | NR | OW | LX | AJ | BQ | CO | QI | NT | | | | ldw hzj | soh wvg |
| 040 | 14 | IV I V | AI | BT | MV | HU | GM | | | | | | | | | imz noa | tjv xtk |
| 040 | 13 | I III II | PW | EL | DO | KN | LY | | | | | | | | | zgr dgr | gjo ryg |
| 040 | 12 | V I | MU | | | | | | | | | | | | | zdy rxf | tjw xtl |
| 040 | 11 | II IV III | RZ | OQ | CP | SX | KN | | | | | | | | | sea rjy | soi vwh |
| 040 | 10 | III V I | | | | | LR | IK | MS | QU | HV | PT | OO | VX | PZ | lrc zbx | vbm rxo |
| 040 | 9 | V I III | | | | | QT | BS | LN | KT | AP | IU | DW | HO | RV | edj eyr | vby tih |
| 040 | 8 | IV II V | | | | | PI | NQ | SY | GU | BE | AH | EL | TX | DO | y | |
| 040 | 7 | I IV II | | | | | UX | IZ | HN | BK | OQ | CP | FT | JY | HW | AR | |
| 040 | 6 | III I V | | | | | DQ | OQ | BW | NP | HK | AZ | CI | PO | JA | YY | |
| 040 | 5 | V II IV | IL | AP | EU | HO | MV | GL | OK | OQ | BI | PU | H5 | PX | HN | EY | |
| 040 | 4 | II IV I | QT | WZ | KV | GM | AC | BL | OZ | EK | QV | OP | SU | DH | JM | TX | lso zby |
| 040 | 3 | V I II | BP | NR | DX | CS | KR | MP | CN | BP | EH | DZ | IW | AV | GJ | LO | lap owd |
| 040 | 2 | IV V I | | | | | BN | HU | EO | PY | KQ | CP | OS | JW | AI | VZ | agd bdy |
| 040 | 1 | III I III | | | | | DP | BM | NZ | CK | OY | HQ | AP | UY | SW | JO | kgl cdf |

$$5 \cdot 4 \cdot 3 \cdot 26^3 \cdot 24! / (12! 2^{12}) \cdot 26! / (10! 6! 2^{10}) \cdot 26^3 \approx 150 \text{ undecillion}$$

The enigma keypspace

Geheime Kommandosache! Jede einzelne Tagesstiftel ist geheim. Mithin: im Flugzeug verboten! Nr. 00190

Luftwaffen-Maschinen-Schlüssel Nr. 649

Achtung! Schlüsselmittel dürfen nicht unversehrt in Feindeshand fallen. Bei Gefahr restlos und fröhzeitig vernichten.

| Tagesstiftel Nr. | Wellenlage | Ringstellung | Städteverbindungen | | | | | | | | | | Benutzgruppen | | | | | |
|---------------------|------------|--------------|----------------------|----|----|----|----|-----------------|----|----|----|----|---------------|----|----|---------|---------|---------|
| | | | an der Blockschleife | | | | | am Stecherbrett | | | | | | | | | | |
| 040 | | 4 06 24 | | | | SZ | GT | DV | KU | FO | MY | EW | JH | IX | LQ | wny dgy | exb rrg | |
| 040 | | 05 26 02 | | | | IS | EV | MX | RW | DT | UZ | JQ | AO | CH | NY | ktl acw | zsl wzo | |
| 040 | | 12 24 03 | KM | AX | PZ | 00 | DJ | AT | CV | IO | ER | QS | LW | PZ | FN | BJ | ioc acn | ovw vvd |
| 040 | 28 | II III V | DI | CH | BR | PV | CR | PV | AI | DK | OT | MQ | EU | BX | LP | GH | lrb cid | ude rzh |
| 040 | 27 | III I IV | LT | EQ | HS | UW | DY | IN | BV | QR | AM | LO | PP | HT | EX | UW | woj fbh | vct uis |
| 040 | 26 | I IV | | | | | VZ | AL | RT | KO | CO | EI | BJ | DU | FS | HP | xle gbo | uev rxm |
| 040 | 25 | IV III | | | | | OR | PV | AD | IT | PK | HJ | LZ | MS | EQ | CW | ouc uhq | uew uit |
| 040 | 24 | V I | | | | | TY | AS | OW | KV | JM | DR | HX | GL | CZ | NU | kpl rwl | vci tlg |
| 040 | 23 | IV III | | | | | QV | FR | AK | EO | DH | CJ | KZ | SX | ON | LT | ebn rwm | udf tlo |
| 040 | 22 | II IV V | IU | AS | DV | GL | PJ | ES | IM | RX | LV | AY | OU | BO | WZ | CN | jqc acx | mwe wvc |
| 040 | 21 | I V II | ET | OX | KZ | CH | RU | HL | PY | OS | GZ | DM | AW | CE | TV | NX | jpw del | mwf wvf |
| 040 | 20 | III IV V | | | | | QZ | AU | RY | SV | JL | OX | BE | TW | | | jgd cef | nvo ysh |
| 040 | 19 | V III I | | | | | PH | WY | DL | CM | AE | TZ | J5 | G1 | | | idf fpx | jwg tlg |
| 040 | 18 | IV II V | | | | | IV | AQ | KW | FX | MT | FS | LU | BD | | | isa gbw | vcj rxn |
| 040 | 17 | I IV II | | | | | FR | EL | LS | EM | OY | OY | QX | AP | JF | BU | mae hti | soE ysi |
| 040 | 16 | V III III | HM | JO | DI | NR | BV | XZ | OS | PU | FQ | CT | | | | | tdp dbh | fkv uiv |
| 040 | 15 | II IV I | DS | HY | NR | OW | LX | AJ | BQ | CO | QI | NT | | | | | ldw hjz | soh wvg |
| 040 | 14 | IV I V | AI | BT | MV | HU | OM | | | | | | | | | | imz noa | tjv xtk |
| 040 | 13 | I III II | PW | EL | DO | KN | LY | | | | | | | | | | zgr dgs | gjo ryg |
| 040 | 12 | V I | MU | | | | | | | | | | | | | | zdy rkf | tjw xtl |
| 040 | 11 | II IV III | RZ | OQ | CP | SX | KN | | | | | | | | | | sea rjy | soi vwh |
| 040 | 10 | III V | | | | | LR | IK | MS | QU | HV | PT | OO | VX | PZ | EN | lrc zbx | vbm rxo |
| 040 | 9 | V I III | | | | | QT | BS | LN | KT | AP | IU | DW | HO | RV | JZ | edj eyr | vby tih |
| 040 | 8 | IV II V | | | | | PI | NQ | SY | GU | BE | AH | EL | TX | DO | KP | y | |
| 040 | 7 | I IV II | | | | | UX | IE | HN | BK | OQ | CP | FT | JY | HW | AR | 1 | |
| 040 | 6 | III I V | | | | | DQ | OQ | BW | NP | HK | AZ | CI | PO | JA | VY | 1 | |
| 040 | 5 | V II IV | IL | AP | EU | HO | MV | GL | OK | OQ | BI | PU | H5 | PX | HN | EY | 1 | |
| 040 | 4 | II IV I | QT | WZ | KV | GM | AC | BL | OZ | EK | QV | OP | SU | DH | JM | TX | 1sb zby | vcy ujb |
| 040 | 3 | V I II | BP | NR | DX | CS | KR | MP | CN | BP | EH | DZ | IW | AV | GJ | LO | lap owd | iwu wak |
| 040 | 2 | IV V I | | | | | BN | HU | EO | PY | KQ | CP | OS | JW | AI | VZ | agd bdy | iyf xtd |
| 040 | 1 | III I III | | | | | DP | BM | NZ | CK | OY | HQ | AP | UY | SW | JO | kgl cdf | giq wuv |

$$5 \cdot 4 \cdot 3 \cdot 26^3 \cdot 24! / (12! 2^{12}) \cdot 26! / (10! 6! 2^{10}) \cdot 26^3 \approx 150 \text{ undecillion}$$

789 decillion

The enigma keypspace

Geheime Kommandosache! Jede einzelne Tageschlüssel ist geheim. Mithin: im Flugzeug verboten! Nr. 00190

Luftwaffen-Maschinen-Schlüssel Nr. 649

Achtung! Schlüsselmittel dürfen nicht unversehrt in Feindeshand fallen. Bei Gefahr restlos und fröhlich vernichten.

| Tagesnummer | Wellenlänge | Ringstellung | Städteverbindungen | | | | | | | | | | Benutzgruppen | | | | | | |
|-------------|-------------|--------------|-----------------------|----|----|----|----|----------------|----|----|----|----|---------------|----|----|-----|-----|-----|-----|
| | | | an der Blockadebrücke | | | | | am Stabsbureau | | | | | | | | | | | |
| 040 | | 4 06 24 | | | | SZ | GT | DV | KU | FO | MY | EW | JH | IX | LQ | wny | dgy | exb | rfg |
| 040 | | 05 26 02 | | | | IS | EV | MX | RW | DT | UZ | JQ | AO | CH | NY | ktl | acw | zsl | wzo |
| 040 | | 12 24 03 | KM | AX | PZ | 00 | DJ | AT | CV | IO | ER | QS | LW | PZ | FN | ljc | acn | ovw | vwd |
| 040 | 28 | II III V | 06 08 16 | | | DI | CH | BR | PV | CR | PV | AI | DK | OT | MQ | EU | BX | LB | HP |
| 040 | 27 | III I IV | 11 03 07 | | | LT | EQ | HS | UW | DY | IN | BV | QR | AM | LO | PP | HT | EX | UW |
| 040 | 26 | I IV | | | | VZ | AL | RT | KO | CO | EI | BJ | DU | FS | HP | xle | gbo | uev | rxm |
| 040 | 25 | IV III | | | | OR | PV | AD | IT | PK | HJ | LZ | NS | EQ | CW | ouc | uhq | uew | uit |
| 040 | 24 | V I | | | | TY | AS | OW | KV | JM | DR | HX | GL | CZ | NU | kpl | rwl | vci | tlq |
| 040 | 23 | IV II | | | | QV | FR | AK | EO | DH | CJ | KZ | SX | ON | LT | ebn | rwm | udf | tlo |
| 040 | 22 | II IV V | 01 09 21 | | | IU | AS | DV | GL | PJ | ES | IM | RX | LV | AY | OU | BO | WZ | CN |
| 040 | 21 | I V II | 13 05 19 | | | ET | OX | KZ | CH | RU | HL | PY | OS | GZ | DM | AW | CE | TV | NX |
| 040 | 20 | III IV V | 24 00 00 | | | QZ | AU | RY | SV | JL | OX | BE | TE | JS | GI | Jqd | cef | nvo | ysh |
| 040 | 19 | V III I | 17 00 00 | | | PH | WY | DL | CM | AE | TZ | J5 | GI | | | idf | fpz | jwg | tig |
| 040 | 18 | IV II V | 15 00 00 | | | IV | AQ | KW | FX | MT | FS | LU | BD | | | isa | gbw | vcj | rxn |
| 040 | 17 | I IV II | 21 10 00 | | | FR | EL | LS | EM | OY | OY | QX | AP | JF | BU | mae | hti | soE | ysi |
| 040 | 16 | V II III | 08 16 13 | | | HM | JO | DI | NR | BV | XZ | OS | PU | FQ | CT | tdp | dhb | fkv | uiv |
| 040 | 15 | II IV I | 01 03 07 | | | DS | HY | NR | OW | LX | AJ | BQ | CO | PI | NT | ldw | hzt | soh | wtg |
| 040 | 14 | IV I V | 15 11 05 | AI | BT | MV | HU | GM | | | | | | | | imz | noa | tjv | xtk |
| 040 | 13 | I III II | 13 20 03 | PW | EL | DO | KN | LY | | | | | | | | sgr | dgz | gjo | ryg |
| 040 | 12 | V I IV | 18 10 07 | MU | | | | KN | | | | | | | | zdy | rkf | tjw | xtl |
| 040 | 11 | II IV III | 02 26 15 | RZ | OQ | CP | SX | | | | | | | | | sea | rjy | soi | whv |
| 040 | 10 | III V I | 23 21 01 | | | | | LR | IK | MS | QU | HV | PT | OO | VX | PZ | EN | | |
| 040 | 9 | V I III | 16 04 08 | | | | | QT | BS | LN | KT | AP | IU | DW | HO | RV | JZ | | |
| 040 | 8 | IV II V | 13 19 25 | | | | | PI | NQ | SY | GU | BE | AH | EL | TX | DO | KP | | |
| 040 | 7 | I IV II | 09 03 22 | | | | | UX | IZ | HN | BK | OQ | CP | FT | JY | HW | AR | | |
| 040 | 6 | III I V | 11 18 14 | | | | | DQ | OQ | BW | NP | HK | AZ | CI | PO | JA | VY | | |
| 040 | 5 | V II IV | 23 02 25 | IL | AP | EU | HO | MV | GL | OK | OQ | BI | PU | H5 | PX | HN | EY | | |
| 040 | 4 | II IV I | 04 21 09 | QT | WZ | KV | GM | AC | BL | OZ | EK | QV | OP | SU | DH | JM | TX | lso | zby |
| 040 | 3 | V I II | 19 11 06 | BP | NR | DX | CS | KR | MP | CN | BP | EH | DZ | IW | AV | GJ | LO | lap | owd |
| 040 | 2 | IV V I | 16 14 02 | | | | | BN | HU | EO | PY | KQ | CP | OS | JW | AI | VZ | agd | bdy |
| 040 | 1 | III I III | 23 12 10 | | | | | DP | BM | NZ | CK | OY | HQ | AP | UY | SW | JO | kgl | edf |

rotors

ring

reflector

plugboard

positions

$$5 \cdot 4 \cdot 3 \cdot 26^3 \cdot 24! / (12! 2^{12}) \cdot 26! / (10! 6! 2^{10}) \cdot 26^3 \approx 150 \text{ undecillion}$$

789 decillion 931 nonillion

The enigma keypspace

Geheime Kommandosache! Jede einzelne Tagesstiftel ist geheim. Mithin: im Flugzeug verboten! Nr. 00190

Luftwaffen-Maschinen-Schlüssel Nr. 649

Achtung! Schlüsselmittel dürfen nicht unversehrt in Feindeshand fallen. Bei Gefahr restlos und fröhzeitig vernichten.

| Tagesstiftel Nr. | Wellenlage | Ringstellung | Ständeverbindungen | | Benutzungsgruppen | |
|---------------------|------------|--------------|--------------------|-------------------------------|-------------------|---------|
| | | | an der Buchstabe | am Stehbeleg | | |
| 040 | | 4 06 24 | | SZ OT DV KU FO MY EW JH IX LQ | wny dgy | exb rrg |
| 040 | | 05 26 02 | | IS EV MX RW DT UZ JQ AO CH NY | ktl acw | zsl wzo |
| 040 | | 12 24 03 | KM AX PZ 00 | DJ AT CV IO ER QS LW PZ FN BH | ioc acn | ovw wsh |
| 040 | 28 | 11 03 07 | DI CH BR PV | CR PV AI DK OT MQ EU BX LH | lrb cid | ude rzh |
| 040 | 27 | 06 08 16 | LT EQ HS UW | DY IH BV QR AM LO PP HT EX UW | woj fbh | vct uis |
| 040 | 26 | 07 09 15 | | VZ AL RT KO CO EI BJ DU FS HP | xle gbo | uev rxm |
| 040 | 25 | 08 16 13 | | OR PV AD IT PK HJ LZ NS EQ CW | ouc uhq | uew uit |
| 040 | 24 | 09 15 02 | | TY AS OW KV JM DR HX GL CZ NU | kpl rwl | vci tlg |
| 040 | 23 | 10 04 01 | | QV FR AK EO DH CJ KE SX ON LT | ebn rwm | udf tlo |
| 040 | 22 | 11 03 07 | IU AS DV GL | PJ ES IM RX LV AY OU BO WZ CN | jqc acx | mwe wvc |
| 040 | 21 | 12 02 01 | ET OX KZ CH | RU HL PY OS GZ DM AW CE TV NX | jpw del | mwf wvf |
| 040 | 20 | 13 05 19 | | QZ AU BV SY JX OL BE TW | jgd cef | nvo ysh |
| 040 | 19 | 14 06 08 | | PH WY DL CM AE TZ JS GI | idf fpx | jwg tlg |
| 040 | 18 | 15 07 06 | | IV AQ KW FX MT PS LU BD | isa gbw | vcj rxn |
| 040 | 17 | 16 04 08 | | FR EL LS EM OV OY QX AP JP BU | mae hti | soE ysi |
| 040 | 16 | 17 05 10 | | HM JO DI NR BV XZ OS PU FQ CT | tdp dbh | fkv uiv |
| 040 | 15 | 18 07 01 | | DS HY NR OW LX AJ BQ CO IP NT | ldw hjz | soh wvg |
| 040 | 14 | 19 08 05 | AI BT MV HU | OM | imz noa | tjv xtk |
| 040 | 13 | 20 09 14 | PW EL DG KN | LY | zgr dgs | gjo ryg |
| 040 | 12 | 21 10 06 | RZ OQ CP SX | MU | zdy rkf | tjw xtl |
| 040 | 11 | 22 11 05 | | KN | sea rjy | soi wvh |
| 040 | 10 | 23 12 04 | | LR IK MS QU HV PT OO VX PZ EN | lrc zbx | vbm rxo |
| 040 | 9 | 24 01 03 | | QT BS LN KT AP IU DW HO RV JZ | edj eyr | vby tih |
| 040 | 8 | 25 02 02 | | PI NQ SY CU BE AH EL TX DO KP | | y |
| 040 | 7 | 26 03 01 | | UX IE HN BK OQ CP FT JY HW AR | | z |
| 040 | 6 | 27 04 00 | | DQ OQ BW NP HK AZ CI PO JX VY | | 1 |
| 040 | 5 | 28 05 00 | IL AP EU HO | MV GL OK OQ BI PU HS PX NN EY | | 1 |
| 040 | 4 | 29 06 00 | QT WZ KV OM | AC BL OZ EK QV OP SU DH JM TX | lso zby | vcy ujb |
| 040 | 3 | 30 07 00 | BP NR DX CS | KR MP CN BP EH DZ IW AV GJ LO | lap owd | iwu wak |
| 040 | 2 | 31 08 00 | | BN HU EO PY KQ CP OS JW AI VZ | agd bdy | iyf xtd |
| 040 | 1 | 01 09 00 | | DP BM NZ CK OY HQ AP UY SW JO | kgl cdf | giq wuv |

$$5 \cdot 4 \cdot 3 \cdot 26^3 \cdot 24! / (12! 2^{12}) \cdot 26! / (10! 6! 2^{10}) \cdot 26^3 \approx 150 \text{ undecillion}$$

789 decillion 931 nonillion 331 octillion

The enigma keypspace

Geheime Kommandosache! Jede einzelne Tagesstiftel ist geheim. Minder im Flugzeug verboten! Nr. 00190

Luftwaffen-Maschinen-Schlüssel Nr. 649

Achtung! Schlüsselmittel dürfen nicht unversehrt in Feindeshand fallen. Bei Gefahr restlos und fröhlich vernichten.

| Tagesstiftel Nr. | Wellenlage | Ringstellung | Stellenverbindungen | | Ringgruppen | |
|---------------------|------------|--------------|---------------------|---|-------------|---------|
| | | | an der Buchstabe | am Stehhebel | | |
| 040 | | 4 09 24 | | SZ GT DV KU FO MY EW JH IX LQ | wny dgy | exb rrg |
| 040 | | 05 26 02 | | IS EV MX RW DT UZ JQ AO CH NY | ktl acw | zsl wzo |
| 040 | | 12 24 03 | KM AX PZ 00 | DJ AT CV IO ER QS LW PZ FN BH | ioc acn | ovw rzh |
| 040 | 28 | 11 03 07 | DI CH BR PV | CR PV AI DK OT MQ EU BS LP | lrb cid | ude rsh |
| 040 | 27 | 06 08 16 | LT EQ HS UW | DY IH BV QR AM LO PP HT EX UW | woj fbh | vct uis |
| 040 | 26 | | | VZ AL RT KO CO EI BJ DU FS HP | xle gbo | uev rxm |
| 040 | 25 | | | OR PV AD IT PK HJ LZ NS EQ CW | ouc uhq | uew uit |
| 040 | 24 | | | TY AS OW KV JM DR HX GL CZ NU | kpl rwi | vci tlg |
| 040 | 23 | | | QV FR AK EO DH CJ KE SX ON LT | ebn rwm | udf tlo |
| 040 | 22 | | | PJ ES IM RX LV AY OU BO WZ CN | jqc acx | mwe wvc |
| 040 | 21 | | | RU HL PY OS GZ DM AW CE TV NX | jpw del | mwf wvf |
| 040 | 20 | | | QZ AU BV SY JX OL BE TW | jgd cef | nvo ysh |
| 040 | 19 | | | PH WY DL CM AE TZ JS GI | idf fpx | jwg tlg |
| 040 | 18 | | | IV AQ KW FX MT PS LU BD | isa gbw | vcj rxn |
| 040 | 17 | | | FR EL LS EM OV OY QX AP JP BU | mae hti | soE ysi |
| 040 | 16 | | | HM JO DI NR BV XZ OS PU FQ CT | tdp dbh | fkv uiv |
| 040 | 15 | | | DS HY NR OW LX AJ BQ CO IP NT | ldw hjz | soh wvg |
| 040 | 14 | | | AI BT MV HU OM | imz noa | tjv xtk |
| 040 | 13 | | | LY | zgr dgs | gjo ryg |
| 040 | 12 | | | MU | zdy rkf | tjw xtl |
| 040 | 11 | | | RZ OQ CP SX KN | sea rjy | soi vwh |
| 040 | 10 | | | LR IK MS QU HW PT OO VX PZ EN | irc zbx | vbm rxo |
| 040 | 9 | | | QT BS LN KT AP IU DW HO RV JZ | edj eyr | vby tih |
| 040 | 8 | | | PI NQ SY GU BE AH EL TX DO KP | | |
| 040 | 7 | | | UX IE HN BK OQ CP FT JY HW AR | | |
| 040 | 6 | | | DQ GU BW NP HK AZ CI PO JX VY | | |
| 040 | 5 | | | MV GL OK OQ BI PU HS PX NW EY | | |
| 040 | 4 | | | QT WZ KV OM AC BL OZ EK QV OP SU DH JM TX | lso zby | vcy ujb |
| 040 | 3 | | | BP NR DX CS KR MP CN BP EH DZ IW AV GJ LO | lap owd | iwu wak |
| 040 | 2 | | | BN HU EO PY KQ CP OS JW AI VZ | agd bdy | iyf xtd |
| 040 | 1 | | | DP BM NZ CK OY HQ AP UY SW JO | kgl cdf | giq wuv |

$5 \cdot 4 \cdot 3 \cdot 26^3 \cdot 24! / (12! 2^{12}) \cdot 26! / (10! 6! 2^{10}) \cdot 26^3 \approx 150$ undecillion
 789 decillion 931 nonillion 331 octillion 314 septillion 839 sextillion

The enigma keypspace

Geheime Kommandosache! Jede einzelne Tagesstiftel ist geheim. Minder im Flugzeug verboten! Nr. 00190

Luftwaffen-Maschinen-Schlüssel Nr. 649

Achtung! Schlüsselmittel dürfen nicht unversehrt in Feindeshand fallen. Bei Gefahr restlos und fröhzeitig vernichten.

| Tagesstiftel Nr. | Wellenlage | Ringstellung | Stellenverbindungen | | Ringgruppen | |
|---------------------|------------|--------------|---------------------|-------------------------------|-------------|---------|
| | | | an der Buchstabe | am Stecherblech | | |
| 040 | | 4 09 24 | | SZ OT DV KU FO MY EW JH IX LQ | wny dgy | exb rrg |
| 040 | | 05 26 02 | | IS EV MX RW DT UZ JQ AO CH NY | ktl acw | zsl wzo |
| 040 | | 12 24 03 | KM AX PZ 00 | DJ AT CV IO ER QS LW PZ FN BH | ioc acn | ovw rzh |
| 040 | 28 | 11 03 07 | DI CH BR PV | CR PV AI DK OT MQ EU BS LP | lrb cid | ude rsh |
| 040 | 27 | 06 08 16 | LT EQ HS UW | DY IH BV QR AM LO PP HT EX UW | woj fbh | vct uis |
| 040 | 26 | 07 09 15 | | VZ AL RT KO CO EI BJ DU FS HP | xle gbo | uev rxm |
| 040 | 25 | 08 16 13 | | OR PV AD IT PK HJ LZ NS EQ CW | ouc uhq | uew uit |
| 040 | 24 | 09 15 02 | | TY AS OW KV JM DR HX GL CZ NU | kpl rwl | vci tlg |
| 040 | 23 | 10 03 07 | | QV FR AK EO DH CJ KE SX ON LT | ebn rwm | udf tlo |
| 040 | 22 | 11 03 07 | IU AS DV GL | PJ ES IM RX LV AY OU BO WZ CN | jqc acx | mwe wvc |
| 040 | 21 | 12 03 07 | ET OX KZ CH | RU HL PY OS GZ DM AW CE TV NX | jpw del | mwf wvf |
| 040 | 20 | 13 05 19 | | QZ AU BV SY JX OL BE TW | jgd cef | nvo ysh |
| 040 | 19 | 14 05 19 | | PH WY DL CM AE TZ JS GI | idf fpx | jwg tlg |
| 040 | 18 | 15 11 05 | | IV AQ KW FX MT PS LU BD | isa gbw | vcj rxn |
| 040 | 17 | 16 04 08 | | FR EL LS EM OV OY QX AP JP BU | mae hti | soE ysi |
| 040 | 16 | 17 04 08 | | HM JO DI NR BV XZ OS PU FQ CT | tdp dbh | fkv uiv |
| 040 | 15 | 18 07 07 | | DS HY NR OW LX AJ BQ CO IP NT | ldw hjz | soh wvg |
| 040 | 14 | 19 03 07 | AI BT MV HU | OM | imz noa | tjv xtk |
| 040 | 13 | 20 03 07 | PW EL DG KN | LY | zgr dgr | gjo ryg |
| 040 | 12 | 21 03 07 | RZ OQ CP SX | MU | zdy rkf | tjw xtl |
| 040 | 11 | 22 03 07 | | KN | sea rjy | soi vwh |
| 040 | 10 | 23 01 01 | | LR IK MS QU HV PT OO VX PZ EN | lrc zbx | vbm rxo |
| 040 | 9 | 24 04 08 | | QT BS LN KT AP IU DW HO RV JZ | edj eyr | vby tih |
| 040 | 8 | 25 01 01 | | PI NQ SY GU BE AH EL TX DO KP | | y |
| 040 | 7 | 26 04 08 | | UX IE HN BK OQ CP FT JY HW AR | | l |
| 040 | 6 | 27 04 08 | | DQ GU BV NP HK AZ CI PO JX VY | | l |
| 040 | 5 | 28 04 08 | IL AP EU HO | MV GL OK OQ BI PU HS PX NW | | l |
| 040 | 4 | 29 04 08 | QT WZ KV OM | AC BL OZ EK QV OP SU DH JM TX | lso zby | vcy ujb |
| 040 | 3 | 30 04 08 | BP NR DX CS | KR MP CN BF EH DZ IW AV GJ LO | lap owd | iwu wak |
| 040 | 2 | 01 03 07 | | BN HU EO PY KQ CP OS JW AI VZ | agd bdy | iyf xtd |
| 040 | 1 | 02 03 07 | | DP BM NZ CK OY HQ AP UY SW JO | kgl cdf | giq wuv |

$5 \cdot 4 \cdot 3 \cdot 26^3 \cdot 24! / (12! 2^{12}) \cdot 26! / (10! 6! 2^{10}) \cdot 26^3 \approx 150$ undecillion
 789 decillion 931 nonillion 331 octillion 314 septillion 839 sextillion
 42 quintillion

The enigma keystore

Geheime Kommandosache! Jede einzelne Tagesstiftel ist geheim. Minder im Flugzeug verboten! Nr. 00190

Luftwaffen-Maschinen-Schlüssel Nr. 649

Achtung! Schlüsselmittel dürfen nicht unversehrt in Feindeshand fallen. Bei Gefahr restlos und fröhlich vernichten.

| Tagesstiftel Nr. | Wellenlage | Ringstellung | Stellscheibenverbindungen | | Ringgruppen | | | |
|---------------------|------------|----------------|---------------------------|-------------------------------|-------------------------------|-------------|---------|---------|
| | | | an der Buchstabe | am Stehscheibe | | | | |
| 040 | | 4 06 24 | | SZ OT DV KU FO MY EW JH IX LQ | wny dgy | exb rrg | | |
| 040 | | 05 26 02 | | IS EV MX RW DT UZ JQ AO CH NY | ktl acw | zsl wzo | | |
| 040 | | 12 24 03 | KM AX PZ 00 | DJ AT CV IO ER QS LW PZ FN BH | ioc acn | ovw rzh | | |
| 040 | | 28 11 06 08 16 | DI CH BR PV | CR PV AI DK OT MQ EU BS LP GJ | lrb cid | ude rwd | | |
| 040 | 28 | III I | IV | 11 03 07 | LT EQ HS UW | woj fbb | vct uis | |
| 040 | 27 | III I | IV | 11 03 07 | | xle gbo | uev rxm | |
| 040 | 26 | I | IV | | VZ AL RT KO CO EI BJ DU FS HP | ouc uhq | uew uit | |
| 040 | 25 | IV | III | | OR PV AD IT PK HJ LZ NS EQ CW | kpl rwi | vci tlg | |
| 040 | 24 | V | I | | TY AS OW KV JM DR HX GL CZ NU | ebn rwm | udf tlo | |
| 040 | 23 | IV | II | | QV FR AK EO DH CJ KE SX ON LT | jqc acx | mwe wvc | |
| 040 | 22 | II | IV | V | 01 09 21 | IU AS DV GL | jpw del | mwf wvf |
| 040 | 21 | I | V | II | 13 05 19 | ET OX KZ CH | jgd cef | nvo ysh |
| 040 | 20 | III | IV | V | 24 06 10 | | idf fpx | jwg tlg |
| 040 | 19 | V | III | I | 17 23 03 | | isa gbw | vcj rxn |
| 040 | 18 | IV | II | V | 15 11 05 | | mae hti | soE ysi |
| 040 | 17 | I | IV | II | 21 10 06 | | tdp dhh | fkb uiv |
| 040 | 16 | V | III | III | 08 16 13 | | ldw hjz | soh wvg |
| 040 | 15 | II | IV | I | 01 03 07 | | imz noa | tjv xtk |
| 040 | 14 | IV | I | V | 15 11 05 | AI BT MV HU | zgr dgs | gjo ryg |
| 040 | 13 | I | III | II | 13 20 03 | PW EL DG KN | zdy rkf | tjw xtl |
| 040 | 12 | V | I | IV | 18 10 07 | MU | sea rjy | soi vwh |
| 040 | 11 | II | IV | III | 02 26 15 | RZ OQ CP SX | lrc zbx | vbm rxo |
| 040 | 10 | III | V | IV | 23 21 01 | | edj eyr | vby tih |
| 040 | 9 | V | I | III | 16 04 08 | | | |
| 040 | 8 | IV | II | V | 13 19 25 | | | |
| 040 | 7 | I | IV | II | 09 03 22 | | | |
| 040 | 6 | III | I | V | 11 18 14 | | | |
| 040 | 5 | V | II | IV | 23 02 25 | IL AP EU HO | lso zby | vcy ujb |
| 040 | 4 | II | IV | I | 04 21 09 | QT WZ KV OM | lap owd | iwu wak |
| 040 | 3 | V | I | II | 19 11 06 | BP NR DX CS | agd bdy | iyf xtd |
| 040 | 2 | IV | V | I | 16 14 02 | | kgl cdf | giq wuv |
| 040 | 1 | II | I | III | 23 12 10 | | | |

rotors

ring

reflector

plugboard

positions

$5 \cdot 4 \cdot 3 \cdot 26^3 \cdot 24! / (12! 2^{12}) \cdot 26! / (10! 6! 2^{10}) \cdot 26^3 \approx 150$ undecillion
 789 decillion 931 nonillion 331 octillion 314 septillion 839 sextillion
 42 quintillion 76 quadrillion

The enigma keypspace

Geheime Kommandosache! Jede einzelne Tagesstiftung ist geheim. Minder im Flugzeug verboten! Nr. 00190

Luftwaffen-Maschinen-Schlüssel Nr. 649

Achtung! Schlüsselmittel dürfen nicht unversehrt in Feindeshand fallen. Bei Gefahr restlos und fröhlich vernichten.

| Tagesstiftung | Wellenlage | Ringstellung | Stellenverbindungen | | Kerngruppen | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---------------|------------|--------------|---------------------|-----|-------------|-------------|----|----|----|----|----|----|----|----|---------|---------|---------|---------|----|----|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|--|--|
| | | | an der Buchstabe | | | am Stehbein | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | | 1 | 2 | | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | | | | | | | | | | | | | | | | | | | |
| 040 | | 4 06 24 | | | SZ | GT | DV | KU | FO | MY | EW | JH | IX | LQ | wny dgy | exb rrg | | | | | | | | | | | | | | | | |
| 040 | | 05 26 02 | | | IS | EV | MX | RW | DT | UZ | JQ | AO | CH | NY | ktl acw | zsl wzo | | | | | | | | | | | | | | | | |
| 040 | | 12 24 03 | KM | AX | PZ | 00 | DJ | AT | CV | IO | ER | QS | LW | PZ | FN | BH | ioc acn | ovw rzd | | | | | | | | | | | | | | |
| 040 | 28 | III | V | 06 | 08 | 16 | DI | CH | BR | PV | CR | PV | AI | DK | OT | MQ | EU | BS | LP | GJ | lrb cid | ude rsh | | | | | | | | | | |
| 040 | 27 | III | I | IV | 11 | 03 | 07 | LT | EQ | HS | UW | DY | IN | BV | QR | AM | LO | PP | HT | EX | UW | woj fbh | vct uis | | | | | | | | | |
| 040 | 26 | I | IV | | | | | | | | | VZ | AL | RT | KO | CO | EI | BJ | DU | FS | HP | xle gbo | uev rxm | | | | | | | | | |
| 040 | 25 | IV | III | | | | | | | | | OR | PV | AD | IT | PK | HJ | LZ | MS | EQ | CW | ouc uhq | uew uit | | | | | | | | | |
| 040 | 24 | V | I | | | | | | | | | TY | AS | OW | KV | JM | DR | HX | GL | CZ | NU | kpl rwl | vci tlg | | | | | | | | | |
| 040 | 23 | IV | II | | | | | | | | | QV | FR | AK | EO | DH | CJ | KE | SX | ON | LT | ebn rwm | udf tlo | | | | | | | | | |
| 040 | 22 | II | IV | V | 01 | 09 | 21 | IU | AS | DV | GL | PJ | ES | IM | RX | LV | AY | OU | BO | WZ | CN | jqc acx | mwe wvc | | | | | | | | | |
| 040 | 21 | I | V | II | 13 | 05 | 19 | PT | OX | KZ | CH | RU | HL | PY | OS | GZ | DM | AW | CE | TV | NX | jpw del | mwf wvf | | | | | | | | | |
| 040 | 20 | III | IV | V | 24 | 00 | | | | | | QE | AU | RY | SV | JL | OX | BE | TW | | | jgd cef | nvo ysh | | | | | | | | | |
| 040 | 19 | V | III | I | 17 | 00 | | | | | | PH | WY | DL | CM | AE | TZ | JS | GI | | | | idf fpx | jwg tlg | | | | | | | | |
| 040 | 18 | IV | II | V | 15 | 00 | | | | | | IV | AQ | KW | FX | MT | FS | LU | BD | | | | isa gbw | vcj rxn | | | | | | | | |
| 040 | 17 | I | IV | II | 21 | 10 | 00 | | | | | FR | EL | LS | EM | OV | OY | QX | AP | JP | BU | | | mae hti | soE ysi | | | | | | | |
| 040 | 16 | V | II | III | 08 | 16 | 13 | | | | | HM | JO | DI | NR | BV | XZ | OS | PU | FQ | CT | | | tdp dbh | fkv uiv | | | | | | | |
| 040 | 15 | II | IV | I | 01 | 03 | 07 | | | | | DS | HY | NR | OW | LX | AJ | BQ | CO | IP | NT | | | | ldw hjz | soh wvg | | | | | | |
| 040 | 14 | IV | I | V | 15 | 11 | 05 | AI | BT | MV | HU | OM | | | | | | | | | | | | | | imz noa | tjv xtk | | | | | |
| 040 | 13 | I | III | II | 13 | 20 | 03 | PW | EL | DO | KN | LY | | | | | | | | | | | | | | | zgr dgs | gjo ryg | | | | |
| 040 | 12 | V | I | | 18 | 10 | 07 | MU | | | | | | | | | | | | | | | | | | | | zdy rkf | tjw xtl | | | |
| 040 | 11 | II | IV | III | 02 | 26 | 15 | RZ | OQ | CP | SX | KN | | | | | | | | | | | | | | | | sea rjy | soi vwh | | | |
| 040 | 10 | III | V | I | 23 | 21 | 01 | | | | | | | | | | | | | | | | | | | | | | lrc zbx | vbm rxo | | |
| 040 | 9 | V | I | III | 16 | 04 | 08 | | | | | | | | | | | | | | | | | | | | | | edj eyr | vby tih | | |
| 040 | 8 | IV | II | V | 13 | 19 | 25 | | | | | | | | | | | | | | | | | | | | | | | y | | |
| 040 | 7 | I | IV | II | 09 | 03 | 22 | | | | | | | | | | | | | | | | | | | | | | | | | |
| 040 | 6 | III | I | V | 11 | 18 | 14 | | | | | | | | | | | | | | | | | | | | | | | | | |
| 040 | 5 | V | II | IV | 23 | 02 | 25 | IL | AP | EU | HO | MV | GL | OK | OQ | BI | PU | H5 | PX | NW | EY | | | | | | | | | | | |
| 040 | 4 | II | IV | I | 04 | 21 | 09 | QT | WZ | KV | OM | AC | BL | OZ | EK | QV | OP | SU | DH | JM | TX | | | | | | | | | | | |
| 040 | 3 | V | I | II | 19 | 11 | 06 | BP | NR | DX | CS | KR | MP | CN | BP | EH | DZ | IW | AV | GJ | LO | | | | | | | | | | | |
| 040 | 2 | IV | V | I | 16 | 14 | 02 | | | | | | | | | | | | | | | | | | | | | | | | | |
| 040 | 1 | II | I | III | 23 | 12 | 10 | | | | | | | | | | | | | | | | | | | | | | | | | |

$5 \cdot 4 \cdot 3 \cdot 26^3 \cdot 24! / (12! 2^{12}) \cdot 26! / (10! 6! 2^{10}) \cdot 26^3 \approx 150$ undecillion
 789 decillion 931 nonillion 331 octillion 314 septillion 839 sextillion
 42 quintillion 76 quadrillion 184 trillion

The enigma keypspace

Geheime Kommandosache! Jede einzelne Tagesstiftel ist geheim. Minder im Flugzeug verboten! Nr. 00190

Luftwaffen-Maschinen-Schlüssel Nr. 649

Achtung! Schlüsselmittel dürfen nicht unversehrt in Feindeshand fallen. Bei Gefahr restlos und fröhlich vernichten.

| Tagesstiftel Nr. | Wellenlage | Ringstellung | Stellenverbindungen | | Ringgruppen | |
|---------------------|------------|--------------|---------------------|---|-------------|---------|
| | | | an der Buchstabe | am Stechen | | |
| 040 | | 4 06 24 | | SZ OT DV KU FO MY EW JH IX LQ | wny dgy | exb rrg |
| 040 | | 05 26 02 | | IS EV MX RW DT UZ JQ AO CH NY | ktl acw | zsl wzo |
| 040 | | 12 24 03 | KM AX PZ 00 | DJ AT CV IO ER QS LW PZ FN BH | ioc acn | ovw rzd |
| 040 | | 28 06 08 16 | DI CH BR PV | CR PV AI DK OT MQ EU BS LP GJ | lrb cid | ude rsh |
| 040 | 28 | III V | LT EQ HS UW | DY IH BV QR AM LO PP HT EX UW | woj fbh | vct uis |
| 040 | 27 | III I IV | | VZ AL RT KO CO EI BJ DU FS HP | xle gbo | uev rxm |
| 040 | 26 | I IV | | OR PV AD IT PK HJ LZ NS EQ CW | ouc uhq | uew uit |
| 040 | 25 | IV III | | TY AS OW KV JM DR HX GL CZ NU | kpl rwl | vci tlg |
| 040 | 24 | V I | | QV FR AK EO DH CJ KE SX ON LT | ebn rwm | udf tlo |
| 040 | 23 | IV III | | PJ ES IM XR LV AY OU BO WZ CN | jqc acx | mwe wvc |
| 040 | 22 | II IV V | 01 09 21 | RU HL PY OS GZ DM AW CE TV NX | jpw del | mwf wvf |
| 040 | 21 | I V | 11 13 05 19 | FT OX KZ CH | zjd cef | nvo ysh |
| 040 | 20 | III IV V | 14 05 19 | QZ AU BY SV JX OL BE TW | jdf fpx | jwg tlg |
| 040 | 19 | V III I | 17 23 03 | PH WY DL CM AE TZ JS GI | isa gbw | vcj rxn |
| 040 | 18 | IV II V | 15 11 05 | IV AQ KW FX MT PS LU BD | mae hti | soE ysi |
| 040 | 17 | I IV II | 21 10 06 | FR EL LS EM OV OY QX AP JP BU | tdp dbh | fkv uiv |
| 040 | 16 | V III III | 08 16 13 | HM JO DI NR BY XZ OS PU FQ CT | ldw hjz | soh wvg |
| 040 | 15 | II IV I | 01 03 07 | DS HY NR OW LX AJ BQ CO IP NT | imz noa | tjv xtk |
| 040 | 14 | IV I V | 15 11 05 | AI BT MV HU OM | zgr dgr | gjo ryg |
| 040 | 13 | I III II | 13 20 03 | PW EL DG KN LY | zdy rkf | tjw xtl |
| 040 | 12 | V I | 18 10 07 | MU | sea rjy | soi vwh |
| 040 | 11 | II IV III | 02 26 15 | RZ OQ CP SX KN | lrc zbx | vbm rxo |
| 040 | 10 | III V | 23 21 01 | LR IK MS QU HV PT 00 VX PZ EN | edj eyr | vby tih |
| 040 | 9 | V I III | 16 04 08 | QT BS LN KT AP IU DW HO RV JZ | y | |
| 040 | 8 | IV II V | 13 19 25 | PI NQ SY GU BE AH EL TX DO KP | 1 | |
| 040 | 7 | I IV II | 09 03 22 | UX IE HN BK OQ CP FT JY HW AR | 1 | |
| 040 | 6 | III I V | 11 18 14 | DQ GU BW NP HK AZ CI PO JX VY | 1 | |
| 040 | 5 | V II IV | 23 02 25 | MV GL OK OQ BI PU HS PX NW EY | 1 | |
| 040 | 4 | II IV I | 04 21 09 | QT WZ KV OM AC BL OZ EK QV OP SU DH JM TX | 1sb zby | vcy ujb |
| 040 | 3 | V I II | 10 11 06 | BP NR DX CS KR MP CN BP EH DZ IW AV GJ LO | lap owd | iwu wak |
| 040 | 2 | IV V I | 16 14 02 | BN HU EO PY KQ CP OS JW AI VZ | agd bdy | iyf xtd |
| 040 | 1 | II III | 23 12 10 | DP BM NZ CK OY HQ AP UY SW JO | kgl cdf | giq wuv |

$5 \cdot 4 \cdot 3 \cdot 26^3 \cdot 24! / (12! 2^{12}) \cdot 26! / (10! 6! 2^{10}) \cdot 26^3 \approx 150$ undecillion
 789 decillion 931 nonillion 331 octillion 314 septillion 839 sextillion
 42 quintillion 76 quadrillion 184 trillion 530 billion

The enigma keypspace

Geheime Kommandosache! Jede einzelne Tagesstiftel ist geheim. Minder im Flugzeug verboten! Nr. 00190

Luftwaffen-Maschinen-Schlüssel Nr. 649

Achtung! Schlüsselmittel dürfen nicht unversehrt in Feindeshand fallen. Bei Gefahr restlos und fröhzeitig vernichten.

| Tagesstiftel Nr. | Wellenlage | Ringstellung | Stellenverbindungen | | Ringgruppen | |
|---------------------|------------|--------------|---------------------|---|-------------|---------|
| | | | an der Buchstabe | am Stecherblech | | |
| 040 | | 4 06 24 | | SZ GT DV KU FO MY EW JH IX LQ | wny dgy | exb rrg |
| 040 | | 05 26 02 | | IS EV MX RW DT UZ JQ AO CH NY | ktl acw | zsl wzo |
| 040 | | 12 24 03 | KM AX PZ 00 | DJ AT CV IO ER QS LW PZ FN BH | ioc acn | ovw rzd |
| 040 | | 22 24 03 | DI CH BR PV | CR PV AI DK OT MQ EU BX LP GJ | lrb cid | ude vsh |
| 040 | 28 | III V | 06 08 16 | DY IH BV QR AM LO PP HT EX UW | woj fbh | vct uis |
| 040 | 27 | III I | IV 11 03 07 | VZ AL RT KO CO EI BJ DU FS HP | xle gbo | uev rxm |
| 040 | 26 | I IV | | OR PV AD IT PK HJ LZ NS EQ CW | ouc uhq | uew uit |
| 040 | 25 | IV III | | TY AS OW KV JM DR HX GL CZ NU | kpl rwl | vci tlg |
| 040 | 24 | V I | | QV FR AK EO DH CJ KE SX ON LT | ebn rwm | udf tlo |
| 040 | 23 | IV III | | PJ ES IM RX LV AY OU BO WZ CN | jqc acx | mwe wvc |
| 040 | 22 | II IV | V 01 09 21 | RU HL PY OS GZ DM AW CE TV NX | jpw del | mwf wvf |
| 040 | 21 | I V | II 13 05 19 | PT OX KZ CH | zjd cef | nvo ysh |
| 040 | 20 | III IV | V 24 05 19 | QZ AU BY SV JX OL BE TW | jdf fpx | jwg tlg |
| 040 | 19 | V III | I 17 23 03 | PH WY DL CM AE TZ JS GI | isa gbw | vcj rxn |
| 040 | 18 | IV II | V 15 11 05 | IV AQ KW FX MT PS LU BD | mae hti | soE ysi |
| 040 | 17 | I IV | II 21 10 06 | FR EL LS EM OV OY QX AP JP BU | tdp dbh | fkv uiv |
| 040 | 16 | V III | III 08 16 13 | HM JO DI NR BY XZ OS PU FQ CT | ldw hjz | soh wvg |
| 040 | 15 | II IV | I 01 03 07 | DS HY NR OW LX AJ BQ CO IP NT | imz noa | tjv xtk |
| 040 | 14 | IV I | V 15 11 05 | AI BT MV HU OM | zgr dgr | gjo ryg |
| 040 | 13 | I III | II 13 20 03 | PW EL DG KN LY | zdy rkf | tjw xtl |
| 040 | 12 | V I | IV 18 10 07 | MU OY QV RZ | sea rjy | soi vwh |
| 040 | 11 | II IV | III 02 26 15 | RZ OQ CP SX KN | lrc zbx | vbm rxo |
| 040 | 10 | III V | IV 23 21 01 | LR IK MS QU HW PT 00 VX PZ EN | edj eyr | vby tih |
| 040 | 9 | V I | III 16 04 08 | QT BS LN KT AP IU DW HO RV JZ | y | |
| 040 | 8 | IV II | V 13 19 25 | PI NQ SY GU BE AH EL TX DO KP | 1 | |
| 040 | 7 | I IV | II 09 03 22 | UX IZ HN BK OQ CP FT JY HW AR | 1 | |
| 040 | 6 | III I | V 11 18 14 | DQ GU BW NP HK AZ CI PO JX VY | 1 | |
| 040 | 5 | V II | IV 23 02 25 | MV GL OK OQ BI PU HS PX NW EY | 1 | |
| 040 | 4 | II IV | I 04 21 09 | QT WZ XV OM AC BL OZ EK QV OP SU DH JM TX | 1sb zby | vcy ujb |
| 040 | 3 | V I | II 19 11 06 | BP NR DX CS KR MP CN BP EH DZ IW AV GJ LO | lap owd | iwu wak |
| 040 | 2 | IV V | I 16 14 02 | BN HU EO PY KQ CP OS JW AI VZ | agd bdy | iyf xtd |
| 040 | 1 | III I | III 23 12 10 | DP BM NZ CK QV HQ AP UY SW JO | kgl edf | giq wuv |

$5 \cdot 4 \cdot 3 \cdot 26^3 \cdot 24! / (12! 2^{12}) \cdot 26! / (10! 6! 2^{10}) \cdot 26^3 \approx 150$ undecillion
 789 decillion 931 nonillion 331 octillion 314 septillion 839 sextillion
 42 quintillion 76 quadrillion 184 trillion 530 billion 944 million

The enigma keystore

Geheime Kommandosache! Jede einzelne Tagesstiftung ist geheim. Minder im Flugzeug verboten! Nr. 00190

Luftwaffen-Maschinen-Schlüssel Nr. 649

Achtung! Schlüsselmittel dürfen nicht unversehrt in Feindeshand fallen. Bei Gefahr restlos und fröhlich vernichten.

| Tagesstiftung | Wolvenlage | Ringstellung | Stellenverbindungen | | Nenngruppen | |
|---------------|------------|--------------|---------------------|---|-------------|---------|
| | | | an der Buchstabe | am Stehbeleg | | |
| 040 | | 4 06 24 | | SZ OT DV KU FO MY EW JH IX LQ | wny dgy | exb rrg |
| 040 | | 05 26 02 | | IS EV MX RW DT UZ JQ AO CH NY | ktl acw | zsl wzo |
| 040 | | 12 24 03 | KM AX PZ 00 | DJ AT CV IO ER QS LW PZ FN BH | ioc acn | ovw rzd |
| 040 | 28 | 11 03 07 | DI CH BR PV | CR PV AI DK OT MQ EU BS LP GJ | lrb cid | ude vsh |
| 040 | 27 | 06 08 16 | LT EQ HS UW | DY IH BV QR AM LO PP HT EX UW | woj fbh | vct uis |
| 040 | 26 | | | VZ AL RT KO CO EI BJ DU FS HP | xle gbo | uev rxm |
| 040 | 25 | IV III | | OR PV AD IT PK HJ LZ NS EQ CW | ouc uhq | uew uit |
| 040 | 24 | V I | | TY AS OW KV JM DR HX GL CZ NU | kpl rwl | vci tlg |
| 040 | 23 | IV III | | QV PR AK EO DH CJ KE SX ON LT | ebn rwm | udf tlo |
| 040 | 22 | II IV V | 01 09 21 | PJ ES IM RX LV AY OU BO WZ CN | jqc acx | mwe wvc |
| 040 | 21 | I V II | 13 05 19 | RU HL PY OS GZ DM AW CE TV NX | jpw del | mwf wvf |
| 040 | 20 | III IV V | 24 06 07 | QZ AU BY SV JX OL BE TW | jgd cef | nvo ysh |
| 040 | 19 | V III I | 17 02 05 | PH WY DL CM AE TZ JS GI | idf fpx | jwg tlg |
| 040 | 18 | IV II V | 15 11 05 | IV AQ KW FX MT PS LU BD | isa gbw | vcj rxn |
| 040 | 17 | I IV II | 21 10 06 | FR EL LS EM OV OY QX AP JP BU | mae hti | soE ysi |
| 040 | 16 | V III III | 08 16 13 | HM JO DI NR BY XZ OS PU FQ CT | tdp dbh | fkv uiv |
| 040 | 15 | II IV I | 01 03 07 | DS HY NR OW LX AJ BQ CO IP NT | ldw hjz | soh wvg |
| 040 | 14 | IV I V | 15 11 05 | AI BT MV HU OM | imz noa | tjv xtk |
| 040 | 13 | I III II | 13 20 03 | PW EL DG KN LY | zgr dgs | gjo ryg |
| 040 | 12 | V I IV | 18 10 07 | MU OX QV RZ | zdy rkf | tjw xtl |
| 040 | 11 | II IV III | 02 26 15 | RZ OQ CP SX KN | sea rjy | soi vwh |
| 040 | 10 | III V I | 23 21 01 | LR IK MS QU HW PT 00 VX PZ EN | irc zbx | vbm rxo |
| 040 | 9 | V I III | 16 04 08 | QT BS LN KT AP IU DW HO RV JZ | edj eyr | vby tih |
| 040 | 8 | IV II V | 13 19 25 | PI NQ SY GU BE AH EL TX DO KP | | |
| 040 | 7 | I IV II | 09 03 22 | UX IE HN BK OQ CP FT JY HW AR | | |
| 040 | 6 | III I V | 11 18 14 | DQ GU BW NP HK AZ CI PO JX VY | | |
| 040 | 5 | V II IV | 23 02 25 | MV GL OK OQ BI PU HS PX NW EY | | |
| 040 | 4 | II IV I | 04 21 09 | QT WZ XV OM AC BL OZ EK QV OP SU DH JM TX | lso zby | vcy ujb |
| 040 | 3 | V I II | 10 11 06 | BP NR DX CS KR MP CN BP EH DZ IW AV GJ LO | lap owd | iwu wak |
| 040 | 2 | IV V I | 16 14 02 | BN HU EO PY KQ CP OS JW AI VZ | agd bdy | iyf xtd |
| 040 | 1 | III I III | 23 12 10 | DP BM NZ CK QV HQ AP UY SW JO | kgl cdf | giq wuv |

rotors

ring

reflector

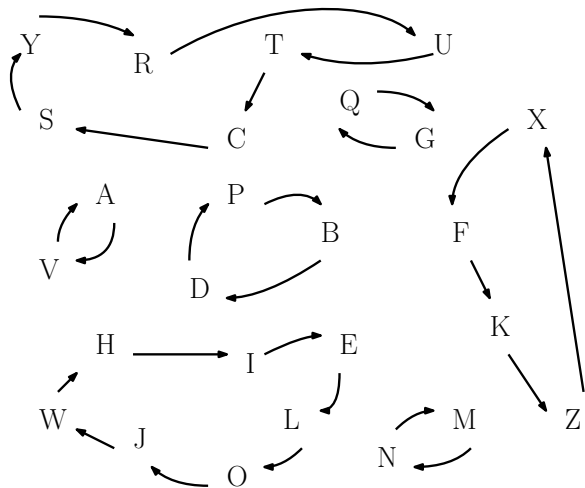
plugboard

positions

$5 \cdot 4 \cdot 3 \cdot 26^3 \cdot 24! / (12! 2^{12}) \cdot 26! / (10! 6! 2^{10}) \cdot 26^3 \approx 150$ undecillion
 789 decillion 931 nonillion 331 octillion 314 septillion 839 sextillion
 42 quintillion 76 quadrillion 184 trillion 530 billion 944 million
 $\approx 10^{38}$ keys

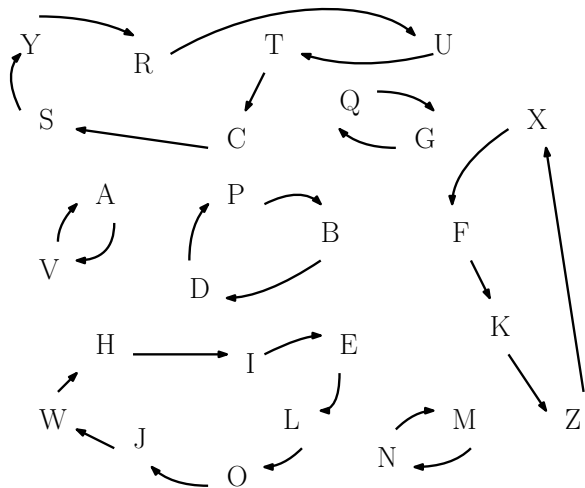
Cryptanalysis of enigma

A random permutation of the alphabet:



Cryptanalysis of enigma

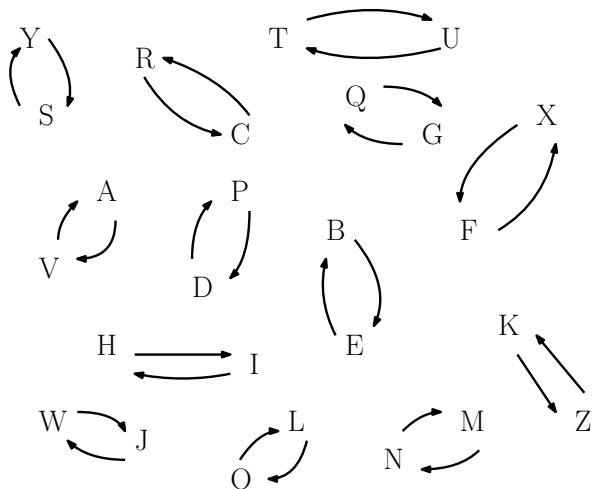
A random permutation of the alphabet:



Cycle structure: 6-2-2-3-4-7-2

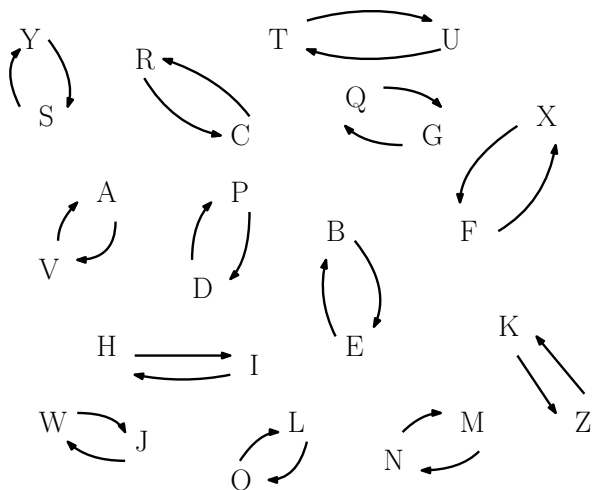
Cryptanalysis of enigma

An enigma permutation of the alphabet:



Cryptanalysis of enigma

An enigma permutation of the alphabet:

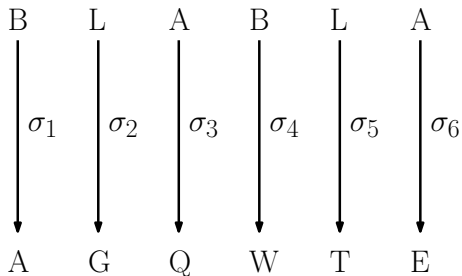


Cycle structure: 2-2-2-2-2-2-2-2-2-2-2-2

Cryptanalysis of enigma

Message key: BLA

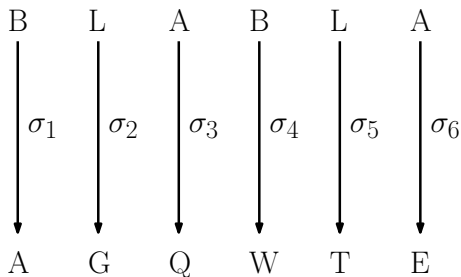
Encrypted message key (using daily key):



Cryptanalysis of enigma

Message key: BLA

Encrypted message key (using daily key):



Learned information about $\sigma_4 \circ \sigma_1$:

$$A \rightarrow W$$

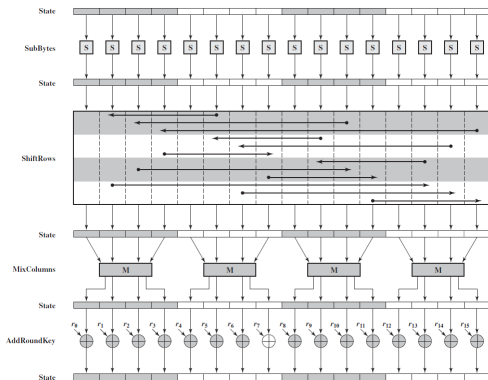
Cryptanalysis of enigma



Bletchley Park Bombe replica

Antoine Taveneaux, CC BY-SA 3.0 <https://creativecommons.org/licenses/by-sa/3.0>, via [Wikimedia Commons](#)

Advent of Computers: AES (Advanced Encryption Standard)



Jeongysu, CC BY-SA 3.0 <https://creativecommons.org/licenses/by-sa/3.0>, via Wikimedia Commons

A new paradigm: public-key cryptography

Sharing secret information across a public channel.

A new paradigm: public-key cryptography

Sharing secret information across a public channel.

Without any setup (no shared secret beforehand).

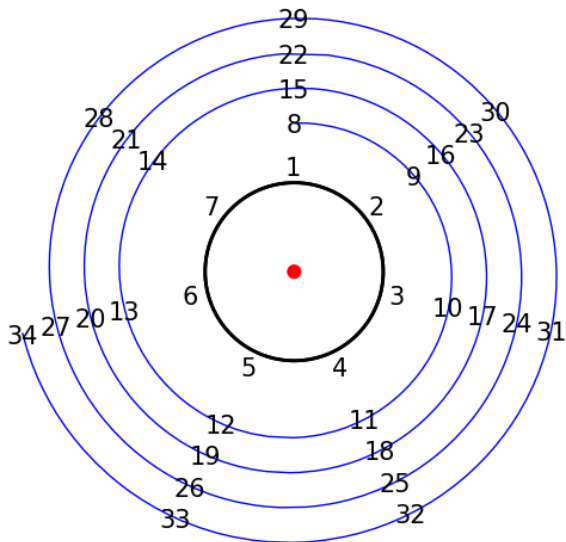
A new paradigm: public-key cryptography

Sharing secret information across a public channel.

Without any setup (no shared secret beforehand).

How is this even possible?!

The door to modern cryptography: modular arithmetic



Diffie-Hellman Key Exchange

Setup: p (modulus), g

Diffie-Hellman Key Exchange

Setup: p (modulus), g

Alice

Bob

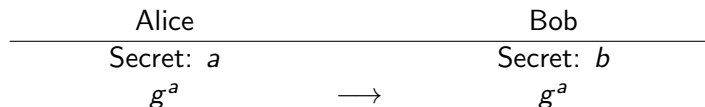
Diffie-Hellman Key Exchange

Setup: p (modulus), g

| | |
|-------------|-------------|
| Alice | Bob |
| Secret: a | Secret: b |

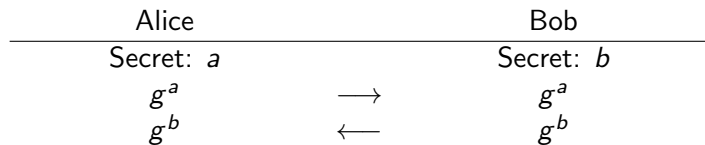
Diffie-Hellman Key Exchange

Setup: p (modulus), g



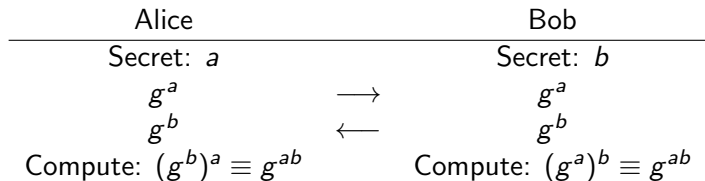
Diffie-Hellman Key Exchange

Setup: p (modulus), g



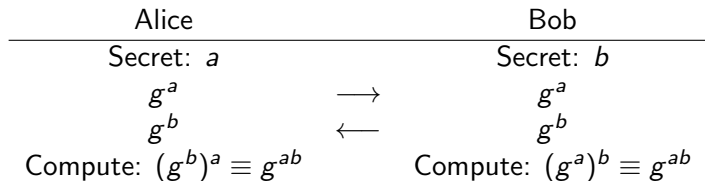
Diffie-Hellman Key Exchange

Setup: p (modulus), g



Diffie-Hellman Key Exchange

Setup: p (modulus), g



An eavesdropper Eve can see g^a and g^b and must compute g^{ab} .

Hard Cryptographic Problems

A **hard cryptographic problem** is:

Hard Cryptographic Problems

A **hard cryptographic problem** is:

- ▶ a mathematical problem (e.g. factoring)

Hard Cryptographic Problems

A **hard cryptographic problem** is:

- ▶ a mathematical problem (e.g. factoring)
- ▶ which is **believed** to be **computationally intensive** to solve,

Hard Cryptographic Problems

A **hard cryptographic problem** is:

- ▶ a mathematical problem (e.g. factoring)
- ▶ which is **believed** to be **computationally intensive** to solve,
- ▶ and upon which we can build a **public-key cryptographic protocol** such as encryption,

Hard Cryptographic Problems

A **hard cryptographic problem** is:

- ▶ a mathematical problem (e.g. factoring)
- ▶ which is **believed** to be **computationally intensive** to solve,
- ▶ and upon which we can build a **public-key cryptographic protocol** such as encryption,
- ▶ whose security is guaranteed by the infeasibility of solving the problem for inputs of a large size.

Hard Cryptographic Problems

A **hard cryptographic problem** is:

- ▶ a mathematical problem (e.g. factoring)
- ▶ which is **believed** to be **computationally intensive** to solve,
- ▶ and upon which we can build a **public-key cryptographic protocol** such as encryption,
- ▶ whose security is guaranteed by the infeasibility of solving the problem for inputs of a large size.

The idea for **public-key encryption** is that

Hard Cryptographic Problems

A **hard cryptographic problem** is:

- ▶ a mathematical problem (e.g. factoring)
- ▶ which is **believed** to be **computationally intensive** to solve,
- ▶ and upon which we can build a **public-key cryptographic protocol** such as encryption,
- ▶ whose security is guaranteed by the infeasibility of solving the problem for inputs of a large size.

The idea for **public-key encryption** is that

- ▶ **encryption** is easy (i.e. fast) using no secret info

Hard Cryptographic Problems

A **hard cryptographic problem** is:

- ▶ a mathematical problem (e.g. factoring)
- ▶ which is **believed** to be **computationally intensive** to solve,
- ▶ and upon which we can build a **public-key cryptographic protocol** such as encryption,
- ▶ whose security is guaranteed by the infeasibility of solving the problem for inputs of a large size.

The idea for **public-key encryption** is that

- ▶ **encryption** is easy (i.e. fast) using no secret info
- ▶ **decryption** is easy **for the intended recipient** (who has extra secret info)

Hard Cryptographic Problems

A **hard cryptographic problem** is:

- ▶ a mathematical problem (e.g. factoring)
- ▶ which is **believed** to be **computationally intensive** to solve,
- ▶ and upon which we can build a **public-key cryptographic protocol** such as encryption,
- ▶ whose security is guaranteed by the infeasibility of solving the problem for inputs of a large size.

The idea for **public-key encryption** is that

- ▶ **encryption** is easy (i.e. fast) using no secret info
- ▶ **decryption** is easy **for the intended recipient** (who has extra secret info)
- ▶ **decryption** is infeasible (i.e. too slow) **for anyone else** (who does not have the extra info)

Hard Cryptographic Problems

A **hard cryptographic problem** is:

- ▶ a mathematical problem (e.g. factoring)
- ▶ which is **believed** to be **computationally intensive** to solve,
- ▶ and upon which we can build a **public-key cryptographic protocol** such as encryption,
- ▶ whose security is guaranteed by the infeasibility of solving the problem for inputs of a large size.

The idea for **public-key encryption** is that

- ▶ **encryption** is easy (i.e. fast) using no secret info
- ▶ **decryption** is easy **for the intended recipient** (who has extra secret info)
- ▶ **decryption** is infeasible (i.e. too slow) **for anyone else** (who does not have the extra info)

For example, to decrypt a message meant for someone else, it may require factoring a number so big, that it is expected to take longer than the length of time before the sun dies.

Warning

We don't actually know they are hard!

Hard Cryptographic Problems

The **Computational Diffie-Hellman Problem**:

Given $g^a, g^b \pmod{p}$, compute g^{ab} .

- ▶ Typical algorithms take around \sqrt{p} time.
- ▶ Human record: p of 795 bits using 3100 core-years
- ▶ Standard internet security: 1024 bits
- ▶ Logjam attack: 512 bits attacked in the wild
- ▶ (Why did Logjam work? Big swaths of the internet were using the **same prime!**)

RSA: Rivest-Shamir-Adelman

The **Factoring Problem**:

Given an integer $n = pq$ for p and q prime, find p and q .

- ▶ Human record: $n \sim 2^{829}$.
- ▶ Standard internet security: $n \sim 2^{2048}$.

How big is 2^{2048} ?

How big is 2^{2048} ?

$2^{2048} =$

Infinity

| | | | | | | |
|-------|-----|----------------|---|---|---|----------|
| Rad | | x! | (|) | % | AC |
| Inv | sin | ln | 7 | 8 | 9 | ÷ |
| π | cos | log | 4 | 5 | 6 | \times |
| e | tan | $\sqrt{\quad}$ | 1 | 2 | 3 | - |
| Ans | EXP | x^y | 0 | . | = | + |

[More info](#)

How big is 2^{2048} ?

Estimate each quantity as a power of two (and put them in order!)

- ▶ The number of atoms in the universe.
- ▶ The number of cells in a human body.
- ▶ The number of insects per human on earth.
- ▶ The number of seconds until the sun dies.

How big is 2^{2048} ?

How big is 2^{2048} ?

- ▶ The number of insects per human on earth: $2^{28} \sim 200$ million.

How big is 2^{2048} ?

- ▶ The number of insects per human on earth: $2^{28} \sim 200$ million.
- ▶ The number of cells in a human body: $2^{45} \sim 37.2$ trillion.

How big is 2^{2048} ?

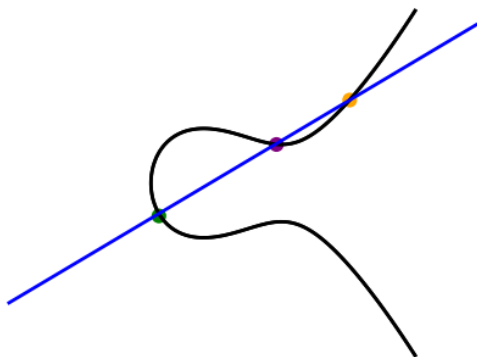
- ▶ The number of insects per human on earth: $2^{28} \sim 200$ million.
- ▶ The number of cells in a human body: $2^{45} \sim 37.2$ trillion.
- ▶ The number of seconds until the sun dies: $2^{57} \sim 7.5$ billion years.

How big is 2^{2048} ?

- ▶ The number of insects per human on earth: $2^{28} \sim 200$ million.
- ▶ The number of cells in a human body: $2^{45} \sim 37.2$ trillion.
- ▶ The number of seconds until the sun dies: $2^{57} \sim 7.5$ billion years.
- ▶ The number of atoms in the universe: $2^{266} \sim 10^{80} \sim 100$ quadrillion vigintillion.

More modern cryptography: Elliptic Curve Cryptography

Do your computations with a crazy group called an



elliptic curve.

The Quantum Age

- ▶ When will we have quantum computers?

The Quantum Age

- ▶ When will we have quantum computers?
 - ▶ The unit of measure is decades.

The Quantum Age

- ▶ When will we have quantum computers?
 - ▶ The unit of measure is decades.
- ▶ What can they do?

The Quantum Age

- ▶ When will we have quantum computers?
 - ▶ The unit of measure is decades.
- ▶ What can they do?
 - ▶ They can factor and solve discrete logarithm too quickly: break all of current cryptography.

The Quantum Age

- ▶ When will we have quantum computers?
 - ▶ The unit of measure is decades.
- ▶ What can they do?
 - ▶ They can factor and solve discrete logarithm too quickly:
break all of current cryptography.
- ▶ What are we doing about it?

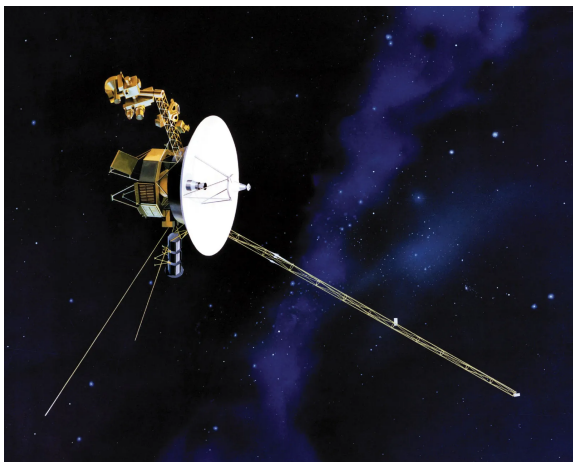
The Quantum Age

- ▶ When will we have quantum computers?
 - ▶ The unit of measure is decades.
- ▶ What can they do?
 - ▶ They can factor and solve discrete logarithm too quickly: break all of current cryptography.
- ▶ What are we doing about it?
 - ▶ NIST is standardizing new protocols based on new hard problems that are believed to be quantum-safe.

The Quantum Age

- ▶ When will we have quantum computers?
 - ▶ The unit of measure is decades.
- ▶ What can they do?
 - ▶ They can factor and solve discrete logarithm too quickly: break all of current cryptography.
- ▶ What are we doing about it?
 - ▶ NIST is standardizing new protocols based on new hard problems that are believed to be quantum-safe.

We will study **quantum cryptography**, **quantum algorithms** and **post-quantum cryptography**.



Bonus: Whirlwind tour of coding theory

Image: the editors of encyclopedia britannica, CC BY-SA 4.0 <https://creativecommons.org/licenses/by-sa/4.0>, via Wikimedia Commons

Coding Theory

- ▶ What is coding theory for? (What problem are we solving?)

Coding Theory

- ▶ What is coding theory for? (What problem are we solving?)
 - ▶ Real-life **channels** (radio, cell phone, copper wires) are **noisy**.

Coding Theory

- ▶ What is coding theory for? (What problem are we solving?)
 - ▶ Real-life **channels** (radio, cell phone, copper wires) are **noisy**.
 - ▶ We want to send messages in such a way that errors won't prevent understanding.

Coding Theory

- ▶ What is coding theory for? (What problem are we solving?)
 - ▶ Real-life **channels** (radio, cell phone, copper wires) are **noisy**.
 - ▶ We want to send messages in such a way that errors won't prevent understanding.
 - ▶ Usually we model a channel as something that randomly flips bits of our binary message (**errors**).

Coding Theory

- ▶ What is coding theory for? (What problem are we solving?)
 - ▶ Real-life **channels** (radio, cell phone, copper wires) are **noisy**.
 - ▶ We want to send messages in such a way that errors won't prevent understanding.
 - ▶ Usually we model a channel as something that randomly flips bits of our binary message (**errors**).
 - ▶ Nothing to do with secrecy.

Coding Theory

- ▶ What is coding theory?

Coding Theory

- ▶ What is coding theory?
 - ▶ We change our message (**encoding**) so that it is error resistant.

Coding Theory

- ▶ What is coding theory?
 - ▶ We change our message (**encoding**) so that it is error resistant.
 - ▶ We send **codewords** instead of plaintext symbols.

Coding Theory

- ▶ What is coding theory?
 - ▶ We change our message (**encoding**) so that it is error resistant.
 - ▶ We send **codewords** instead of plaintext symbols.
 - ▶ Example: 'Victor' instead of 'V' (radio) or '000' instead of '0' (a repeat code)

Coding Theory

- ▶ What is coding theory?
 - ▶ We change our message (**encoding**) so that it is error resistant.
 - ▶ We send **codewords** instead of plaintext symbols.
 - ▶ Example: 'Victor' instead of 'V' (radio) or '000' instead of '0' (a repeat code)
 - ▶ The receiver must **decode**

Coding Theory

- ▶ What makes a good code?

Coding Theory

- ▶ What makes a good code?
 - ▶ Strong **error correction**: the number of errors a codeword can absorb and still be guessed correctly (e.g. '010' is probably '0' not '1')

Coding Theory

- ▶ What makes a good code?
 - ▶ Strong **error correction**: the number of errors a codeword can absorb and still be guessed correctly (e.g. '010' is probably '0' not '1')
 - ▶ Strong **efficiency**: not too much space inflation (codewords are longer than the symbols they represent)
- ▶ What math goes into it?

Coding Theory

- ▶ What makes a good code?
 - ▶ Strong **error correction**: the number of errors a codeword can absorb and still be guessed correctly (e.g. '010' is probably '0' not '1')
 - ▶ Strong **efficiency**: not too much space inflation (codewords are longer than the symbols they represent)
- ▶ What math goes into it?
 - ▶ Finite fields, linear algebra

Your semester ahead

- ▶ About me: a number theorist and cryptographer (cryptanalyst mostly) studying post-quantum cryptography, elliptic-curve cryptography etc.

Your semester ahead

- ▶ About me: a number theorist and cryptographer (cryptanalyst mostly) studying post-quantum cryptography, elliptic-curve cryptography etc.
- ▶ Course modules:
 - ▶ Paradigms, history and application
 - ▶ Modular arithmetic & discrete logarithm
 - ▶ Euclidean algorithm, primality testing & factoring
 - ▶ Finite fields & elliptic curve cryptography
 - ▶ Coding theory & lattice-based cryptography
 - ▶ Quantum aspects

Your semester ahead

- ▶ About me: a number theorist and cryptographer (cryptanalyst mostly) studying post-quantum cryptography, elliptic-curve cryptography etc.
- ▶ Course modules:
 - ▶ Paradigms, history and application
 - ▶ Modular arithmetic & discrete logarithm
 - ▶ Euclidean algorithm, primality testing & factoring
 - ▶ Finite fields & elliptic curve cryptography
 - ▶ Coding theory & lattice-based cryptography
 - ▶ Quantum aspects
- ▶ Course style: **Daily assignments**, regular quizzes, poster project, self-evaluation

Your semester ahead

- ▶ About me: a number theorist and cryptographer (cryptanalyst mostly) studying post-quantum cryptography, elliptic-curve cryptography etc.
- ▶ Course modules:
 - ▶ Paradigms, history and application
 - ▶ Modular arithmetic & discrete logarithm
 - ▶ Euclidean algorithm, primality testing & factoring
 - ▶ Finite fields & elliptic curve cryptography
 - ▶ Coding theory & lattice-based cryptography
 - ▶ Quantum aspects
- ▶ Course style: **Daily assignments**, regular quizzes, poster project, self-evaluation
- ▶ <https://crypto.katestange.net> (linked in canvas) / discord

Your semester ahead

- ▶ About me: a number theorist and cryptographer (cryptanalyst mostly) studying post-quantum cryptography, elliptic-curve cryptography etc.
- ▶ Course modules:
 - ▶ Paradigms, history and application
 - ▶ Modular arithmetic & discrete logarithm
 - ▶ Euclidean algorithm, primality testing & factoring
 - ▶ Finite fields & elliptic curve cryptography
 - ▶ Coding theory & lattice-based cryptography
 - ▶ Quantum aspects
- ▶ Course style: **Daily assignments**, regular quizzes, poster project, self-evaluation
- ▶ <https://crypto.katestange.net> (linked in canvas) / discord
- ▶ contingency plan: last-minute modality change

Your semester ahead

- ▶ About me: a number theorist and cryptographer (cryptanalyst mostly) studying post-quantum cryptography, elliptic-curve cryptography etc.
- ▶ Course modules:
 - ▶ Paradigms, history and application
 - ▶ Modular arithmetic & discrete logarithm
 - ▶ Euclidean algorithm, primality testing & factoring
 - ▶ Finite fields & elliptic curve cryptography
 - ▶ Coding theory & lattice-based cryptography
 - ▶ Quantum aspects
- ▶ Course style: **Daily assignments**, regular quizzes, poster project, self-evaluation
- ▶ <https://crypto.katestange.net> (linked in canvas) / discord
- ▶ contingency plan: last-minute modality change
- ▶ recording class