$x \equiv 3 \pmod{244}$
$x \equiv 17 \pmod{495}$

$244 \cdot 495 = 120780$

① Solve $244s + 495t = 1$.

E.E.A.

$495 = 2 \cdot 244 + 7$

$244 = 34 \cdot 7 + 6$

$7 = 1 \cdot 6 + 1$ ← gcd

E.A.

$495 = 2 \cdot 244 + 7$

$495 \quad s=0 \quad t=1$ $= 2 \cdot$ $244 \quad s=1 \quad t=0$ $+$ $7 \quad s=-2 \quad t=1$

$244 = 34 \cdot 7 + 6$

$244 \quad s=1 \quad t=0$ $= 34 \cdot$ $7 \quad s=-2 \quad t=1$ $+$ $6 \quad s=69 \quad t=-34$

$7 = 1 \cdot 6 + 1$

$7 \quad s=-2 \quad t=1$ $= 1 \cdot$ $6 \quad s=69 \quad t=-34$ $+$ $1 \quad s=-71 \quad t=35$

② $x = 3(495t) + 17(244s)$

$= 51975 - 294508$

$= -242533$

$\equiv -973$

Check:

$244s + 495t$

$= -17324 + 17325$

$= 1$

s, t

Modular Arithmetic Examples

⊙ $2x \equiv 4 \pmod 5$

↑

2 is invertible mod 5

$\Rightarrow$ expect 1 solution

Method 1: Compute 2^{-1}

Then $x \equiv 4(2^{-1}) \pmod 5$

Method 2: Interpret as a linear Dioph. eqⁿ:

$2x = 4 + 5y \quad x \in \mathbb{Z}$

$2x - 5y = 4$

Solve using Eucl. alg: $\gcd(2,5) = 1$

① Find $2x_0 - 5y_0 = 1$] Note: this computes $2^{-1} \bmod 5$

② Multiply solⁿ by 4:

$2(4x_0) - 5(4y_0) = 4$

① Solve $2x \equiv 4 \pmod 6$

2 is not invertible mod 6
$\Rightarrow$ multiple solutions or no solutions

Solution: $2x = 4 + 6y$ in $\mathbb{Z}$

$x = 2 + 3y$

$x \equiv 2 \pmod 3$

$x \equiv 2, 5 \pmod 6$ (2 solutions)

$\mathbb{Z}/6\mathbb{Z}$

3 4 5
0 1 2
↓ ↓ ↓
0 1 2

$\mathbb{Z}/3\mathbb{Z}$

$g = 2 = \gcd(2,6)$
$b = 4$

General Principle

Let $g = \gcd(a,n)$

$ax \equiv b \pmod n$

(A) If $g \mid b$ then,

$ax \equiv b \pmod n$

$\Updownarrow$

$(\frac{a}{g})x \equiv (\frac{b}{g}) \pmod{\frac{n}{g}}$ (*)

① Solve (*)
② Lift solutions to $\mathbb{Z}/n\mathbb{Z}$.

(B) If $g \nmid b$ then no solutions.

$\underbrace{ax - yn}_{\text{div. by } g} = \underbrace{b}_{\text{not}}$

RSA Algorithm

Alice

(n, e)

plaintext message:
$m \pmod n$

Encryption:

$c \equiv m^e \pmod n$

(n, e)

c

Bob

Key Generation:

choose secret primes p, q
choose secret d invertible
mod $\varphi(pq) = (p-1)(q-1)$
and its inverse e.

Public Key: $(n = pq, e)$ ← "encryption exponent"
Private Key: p, q, d ← "decryption exponent"

Decryption:

$c^d \pmod n$
$\equiv m^{ed} \equiv m^1 \equiv m$

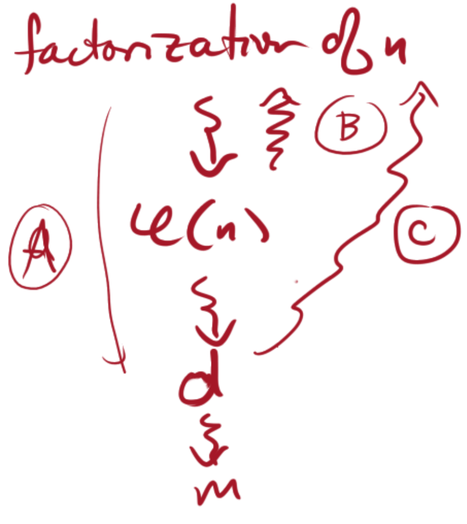
① Eve's Problem (Breaking RSA)

Given $n = pq$

e

$c = m^e \pmod n$

Find m



(A) If Eve factors n, gets p, q.

Compute $\varphi(n) = \varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1)$.

Then compute $d = e^{-1} \pmod{\varphi(n)}$ (Eucl. Alg. solve $ex \equiv 1 \pmod{\varphi(n)}$, $ex + \varphi(n)y = 1$)

Then compute $c^d \pmod m$. That's m.

If we can factor, we can break RSA

(B) If Eve obtains $\varphi(n)$, she can factor n.

$$n - \varphi(n) + 1 = pq - (p-1)(q-1) + 1$$
$$= p + q$$

So $X^2 - (n - \varphi(n) + 1)X + n$
$= X^2 - (p+q)X + pq$
$= (X-p)(X-q)$

has roots p, q.

Use Quadratic Fmla, get p, q.

$n, \varphi(n)$
$\Leftrightarrow$
$(pq, p+q)$

"RSA modulus"
=
n is a product of 2 primes

© If Eve obtains d, she can factor n.

$de \equiv 1 \pmod{\varphi(n)}$

$\varphi(n) \mid de - 1.$

(Euler's Thm)

So $a^{de-1} \equiv 1 \pmod{n}$

Apply Miller-Rabin primality test w/ $de-1$ instead of $n-1$.

Write $de - 1 = 2^k m$, m odd.

Compute chain mod n

$$a^m \longrightarrow a^{2m} \longrightarrow a^{4m} \longrightarrow \cdots \longrightarrow 1$$

Look for ($\rightrightarrows 1$) i.e. $a^{2^l m} \not\equiv \pm 1$

but $a^{2^{l+1} m} \equiv 1$

$\Longrightarrow$ Basic Ppl gives a factor of n.

Cryptographic Size

Record:
829-bit RSA modulus factored in February

NIST, 2015:

2048-bit RSA moduli (for privacy until 2030)

3072-bit for longer.