1. RSA.

(a) Numerization key.

A	B	C	D	E	F	G	H	I	J	K	L	M
11	12	13	14	15	16	17	18	19	20	21	22	23
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
24	25	26	27	28	29	30	31	32	33	34	35	36

(b) Encoding. To compute $n^k \pmod m$:

- **Step 1.** Compute the binary expansion of k (write k as a sum of powers of 2, including, if necessary, the power $2^0 = 1$).
- **Step 2.** Make a list of the base n raised to successive powers of 2 (starting with $2^0 = 1$), $\pmod m$. Keep going until you've raised n to the largest power of 2 appearing in Step 1. Each entry in the list is found by squaring, and reducing $\pmod m$, the previous entry.
- **Step 3.** Put Steps 1 and 2 together to compute $n^k \pmod m$, reducing along the way to keep numbers small.

(c) Decoding. To decode the message b:

- **Step 1.** Find natural numbers x and y such that

$$kx - \varphi(m)y = 1.$$

(See item 3, "The Euclidean Algorithm," below.)

- **Step 2.** Compute $b^x \pmod m$: the result *is* the original message n.

---

2. GCD by factoring.

To find the gcd (greatest common divisor) of two natural numbers a and b:

- **Step 1.** Factor both a and b into products of powers of primes.
- **Step 2.** Take the largest power of each prime that divides both a and b, take the product of these powers, and the result is $\gcd(a, b)$.

---

3. Euclidean Algorithm.

(a) To find the gcd (greatest common divisor) of two natural numbers a and b:

- **Step 1.** Divide the smaller of these two numbers into the larger.
- **Step 2.** Divide the remainder from the previous step into the divisor from the previous step.
- **Step 3.** Repeat Step 2 until you obtain a remainder of zero.
- **Step 4.** When this happens, the previous remainder **is** $\gcd(a, b)$.

(b) To find integers x and y such that $ax - by = 1$:

- **Step 1.** Take the next-to-last of the "remainder equations" that you produced in finding $\gcd(a, b)$, and solve this equation for its remainder (which, again, is $\gcd(a, b)$).
- **Step 2.** Solve the previous remainder equation for the remainder there, and plug this result into the formula just derived for $\gcd(a, b)$. Then simplify by collecting like terms.
- **Step 3.** Repeat Step 2 until you're done.