

Euler: Define $\varphi(n) = \#$ of $\#^s \leq n$ that are relatively prime to n .

Thm: If $n \geq 1$ and $\gcd(a, n) = 1$, then $a^{\varphi(n)} \pmod n = 1$.

Thm: If p is prime, then

- $\varphi(p) = p - 1$
- $\varphi(p^k) = p^k - p^{k-1}$.

Thm: If $\gcd(m, n) = 1$, then $\varphi(mn) = \varphi(m) \cdot \varphi(n)$.

$$\begin{aligned}\underline{\text{Ex:}} \quad \varphi(4800) &= \varphi(2^6 \cdot 3 \cdot 5^2) \\ &= \varphi(2^6) \cdot \varphi(3) \cdot \varphi(5^2) \\ &= (2^6 - 2^5) \cdot (2) \cdot (5^2 - 5^1) \\ &= 32 \cdot 2 \cdot 20 \\ &= 1280.\end{aligned}$$

RSA encryption.

Phase I: Pick two primes $p + q$ $(a, 17)$
 ~~$(2a, 17)$~~

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

Call this number n .

$$n = 15 \cdot 16 \\ = 288$$

Thm: $a^{\varphi(pq)} \% pq = 1$

$$\varphi(pq) = n$$

$$a^n \% pq = 1.$$

Publish ~~n~~ ^{pq} and e

where e is any number relatively prime to n .

Let M be a message.

To encrypt M , compute $M^e \bmod n$.

Phase II: To decrypt, raise the encrypted message to the d^{th} power, where d is e 's multiplicative inverse mod n .

To find d , use the Euclidean Algorithm, and its "reverse unfolding" to find an inverse of e . Call it d .

Decryption

$$(M^e)^d = M^{e \cdot d}$$
$$e \cdot d \bmod n = 1$$
$$\text{so } M^{e \cdot d} \bmod n = M^1 \bmod n$$