Solve $x^a \equiv b \pmod m$

eg $x^7 \equiv 2 \pmod{11}$

$x = \sqrt[7]{2} = 2^{\frac{1}{7}} \pmod{11}$ $\varphi(p) = p-1$ (prime)

$y = 7^{-1} \pmod{\varphi(m)}$ $\varphi(11) = 10$

$7y \equiv 1 \pmod{10}$

$y \equiv 3 \pmod{10}$

$x = b^y = 2^3 \pmod{11} \equiv 8 \pmod{11}$

k	$8^k \pmod{11}$
1	8
2	9
4	4
7	2

WTS $8^7 \equiv 2 \pmod{11}$

$\varphi(11) = 10$

$(8^7)^3 = 8^{21} = 8^{2 \cdot 10 + 1} = 8^{2 \cdot 10} \cdot 8 \equiv 8 \pmod{11}$.

$\therefore 8^7 \equiv 2 \pmod{11}$

RSA algorithm

- Randomly pick large primes p, q, let $n = p \times q$.
- Calculate $\phi(n) = (p-1) \times (q-1)$. Don't tell anyone.
- Choose e with $1 < e < \phi(n)$ coprime to $\phi(n)$.
- Compute d such that $e \cdot d \equiv_{\phi(n)} 1$.
- Public key is (n, e).
- Private key is (n, d).
- Message is m where $0 \leq m < n$.
- Encoding: $m \mapsto m^e \bmod n$.
- Decoding: $c \mapsto c^d \bmod n$.

inverse of e

message.

quite quickly.

crypted.

$Dec(Enc(m)) = Dec(m^e \bmod n) = (m^e)^d \bmod n = m^{e \cdot d} \bmod n = m$.

Multiplicative Group.

$G_m^* = \{a \mid \{1 \le a < m\} \wedge (\gcd(a,m) = 1)\}$

1) Solve $a * y \equiv 1 \pmod m$ in poly time

2) Solve $a^n \pmod m$

$2^{27} \pmod{123}$ $\quad 123 = 3 \times 41$

$\varphi(123) = (123) \times \left(\frac{2}{3}\right) \times \left(\frac{40}{41}\right)$
$= 82 \times \frac{40}{41} = 80$

$2^9 \equiv 256 \equiv 10 \pmod{123}$

$2^{10} \equiv 100 \pmod{123}$

$2^{24} \equiv 1000 \pmod{123} \equiv 16 \pmod{123}$

$2^{27} \equiv 16 \times 8 \pmod{123}$
$\equiv 128 \pmod{123}$
$\equiv 5 \pmod{123}$

3) Solve $x^a \equiv b \pmod m$

$x^3 \equiv 2 \pmod{11}$

$x \equiv \sqrt[3]{2} \equiv 2^{3^{-1}}$

$y = 3^{-1} \pmod{\varphi(11)}$
$\equiv 3^{-1} \pmod{10}$

$\therefore 3^4 \equiv 1 \pmod{10}$

$\therefore y = 3^3 \pmod{10}$
$= 7. \pmod{10}$

$x = 2^7 = 128 = 7 \pmod{11}$

for R^* $x = \sqrt[a]{b} = b^{(a^{-1})}$

$(a, \varphi(m)) = 1$

$a * y = 1 \pmod{\varphi(m)}$

$x = b^y \pmod m$

$x^a = (b^y)^a = b^{ya} = b^{1 + \varphi(m) \cdot k} = b \pmod m$

4) $a^x = b \pmod m$

$7^x \equiv 13 \pmod{15}$

$\varphi(15) = 15 \times (1 - \frac{1}{3}) \times (1 - \frac{1}{5})$
$= 10 \times \frac{4}{5} = 8.$

2. $7^4 \equiv 1 \pmod{15}$ $\Leftarrow$ $\gcd(7, 15) = 1$.

$\therefore$ $x = 8 \times 13 = 104$

$\downarrow$

104

The point of having RSA.

Before:

The encrypt/decrypt machine is a SECRET.
ENIGMA. / BOND

The keys are a BIG SECRET

Math: simply permute all possibilities

After:

The procedure is known to ALL.
running poly time.

The public keys are known to ALL.

Only private key is still SECRET.

Math: f^{-1}: discrete logarithm

f: direct action to compute $a^x \pmod m$ can be done in poly time.

$\uparrow$

encryption