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.

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