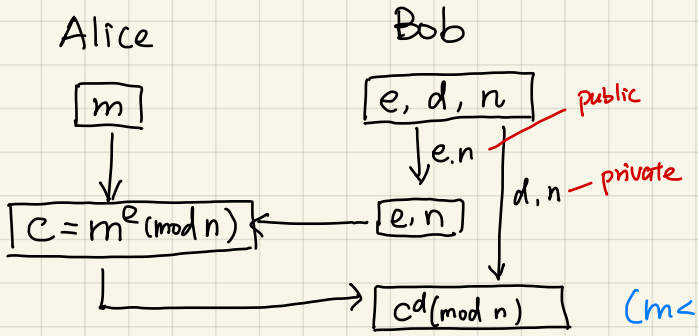
RSA

public-key encryption

communication

message.
encryption exponent
decryption exponent
ciphertext



computation

1. $n = p \cdot q$. $\varphi = (p-1)\cdot(q-1)$ → Euler's Totient Function
2. random e, s.t. $1<e<\varphi$, $\gcd(e,\varphi)=1$. $(e=65537)$
3. compute d, s.t. $ed \equiv 1 \pmod \varphi$

$ed = r\varphi + 1 \Rightarrow ed - r\varphi = 1 = \gcd(e,\varphi) = \gcd(e,-\varphi)$

Bézout's Identity: $\gcd(a,b)=c \Rightarrow \exists x, y$, s.t. $xa+yb=c$

- $\gcd(a,b) = \gcd(b, a \bmod b) = \cdots \Rightarrow b=0$, terminate, output a.
- $\gcd(a,b) = xa+yb$. output $(\gcd, x, y)$

basis: $b=0$, $\Rightarrow x=1$, $y=0$, output $(a, 1, 0)$

induction: $\gcd(a,b) = xa+yb = \gcd(b, a \bmod b) = x'b + y'(a \bmod b)$

let $r = \lfloor \frac{a}{b} \rfloor \Rightarrow a \bmod b = a - rb$. $\Rightarrow = xb + y'(a-rb) = y'a + (x' - ry')b$

$\Rightarrow x = y'$. $y = x' - ry'$.

Theory. **hardness**. $n = p \cdot q$, φ is unknown. $\Rightarrow ed - r\varphi = 1$. hard to compute d.

correctness.

$$c^d \bmod n = (m^e \bmod n)^d \bmod n = m^{ed} \bmod n \overset{?}{\equiv} m \pmod n$$

$(a \cdot b) \bmod p = [(a \bmod p)\cdot(b \bmod p)] \bmod p$

Fermat's Theorem: If p is prime, $\gcd(a,p)=1$, then $a^{p-1} \equiv 1 \pmod p$

case 1. $\gcd(m,p)=1 \Rightarrow m^{p-1} \equiv 1 \pmod p$

$$\left(m^{(p-1)}\right)^{r(q-1)} \cdot m \equiv 1^{r(q-1)} \cdot m \pmod p \equiv m \pmod p$$

$$\Rightarrow m^{r(p-1)\cdot(q-1)+1} = m^{r\varphi+1} = m^{ed}$$

$$\Rightarrow m^{ed} \equiv m \pmod p.$$

case 2. $\gcd(m,p)=p \Rightarrow m^{ed} \pmod p \equiv m \pmod p \equiv 0$

similarly, $\begin{cases} m^{ed} \equiv m \pmod p. \Rightarrow \exists k_1, \text{ s.t } m^{ed} = k_1 \cdot p + m \\ m^{ed} \equiv m \pmod q. \Rightarrow \exists k_2, \text{ s.t } m^{ed} = k_2 \cdot q + m \end{cases}$

$\Rightarrow k_1 \cdot p = k_2 \cdot q \Rightarrow \exists k_3$. s.t. $k_1 = k_3 \cdot q$

$\Rightarrow m^{ed} = k_3 \cdot pq + m \equiv m \pmod{pq} \equiv m \pmod n$