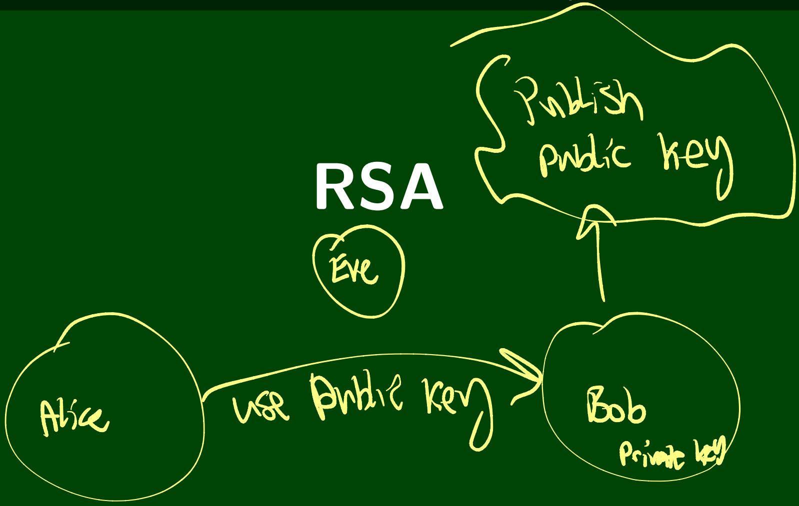
CS 13

Mathematical Foundations of Computer Science

RSA



Public

$n = pq$

$e = 65537$

Private

p, q

d

$\phi(n) = (p-1)(q-1)$

$ed \equiv_{\phi(n)} 1$

(1) Generate two primes p, q $n = pq$

Encrypt

$m^e \bmod n = c$

Decrypt

$c^d \bmod n = m \bmod n$

$$\boxed{ed \equiv_{\phi(n)} 1} \Rightarrow ed = \phi(n)k' + 1$$

$$ed + \phi(n)k = 1$$

$$(m^e \bmod n)^d \bmod n = m^{ed} \bmod n = m^{\phi(n)k'+1} \bmod n$$

$$= m \cdot m^{k'\phi(n)} \bmod n$$

$$m^{k'\phi(n)} = 1$$

$$\boxed{m^{\phi(n)} \equiv_n 1}$$

assumption (prove later)

$$= m \bmod n$$

$\phi(n)$ = the # of numbers $< n$ that and ≥ 1 are <u>relatively prime</u> to n

$\gcd(n, \_) = 1$

$\mathbb{Z}_n^* = \{ x : 1 \leq x < n \wedge \gcd(n, x) = 1 \}$

$\phi(n) = |\mathbb{Z}_n^*|$

$\phi(p) = p - 1$

$\uparrow$ prime

$\phi(pq) = (p-1)(q-1)$

$\uparrow\uparrow$ prime

$ed \equiv_{\phi(n)} 1$

Another Theorem

Cancellation Property $\equiv_n$

If $\gcd(c,n)=1$, then

$$ca \equiv_n cb \implies a \equiv_n b$$

.

Proof.

Since $\gcd(c,n)=1$, it follows that there exists a c^{-1} such that $cc^{-1}+kn=1$ for some $k \in \mathbb{Z}$.

Cancellation Property $\equiv_n$

If $\gcd(c,n) = 1$, then

$$ca \equiv_n cb \implies a \equiv_n b$$

.

Proof.

Since $\gcd(c,n) = 1$, it follows that there exists a c^{-1} such that $cc^{-1} + kn = 1$ for some $k \in \mathbb{Z}$.

$$\begin{aligned}
ca &\equiv_n cb \\
c^{-1}ca &\equiv_n c^{-1}cb && \text{[Multiplying both sides by } c^{-1}\text{]} \\
(1-kn)a &\equiv_n (1-kn)b && \text{[Definition of } c^{-1}\text{]} \\
a + kna &\equiv_n b + knb \\
a &\equiv_n b && [knX \equiv_n 0]
\end{aligned}$$