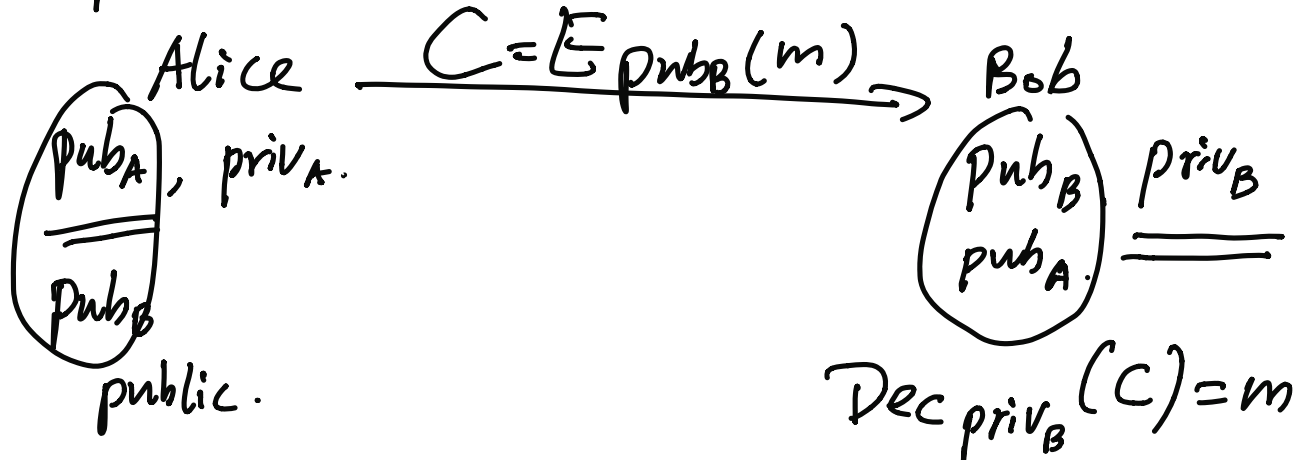


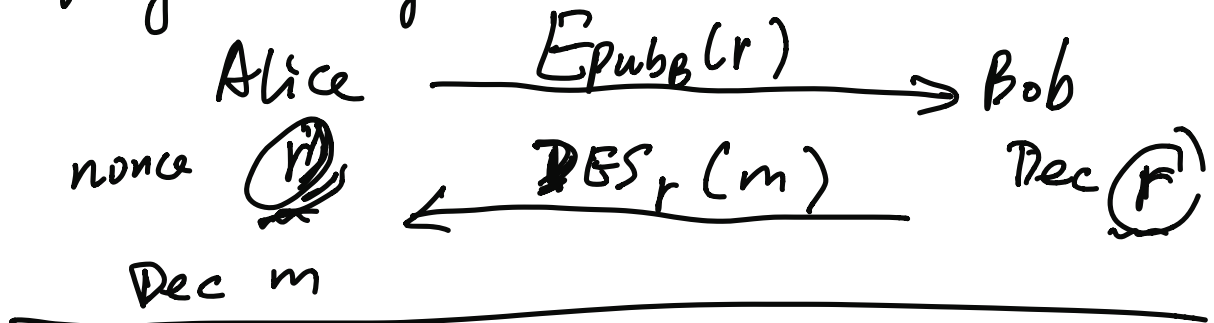
ECE 471/571

Public key crypto (PKC)

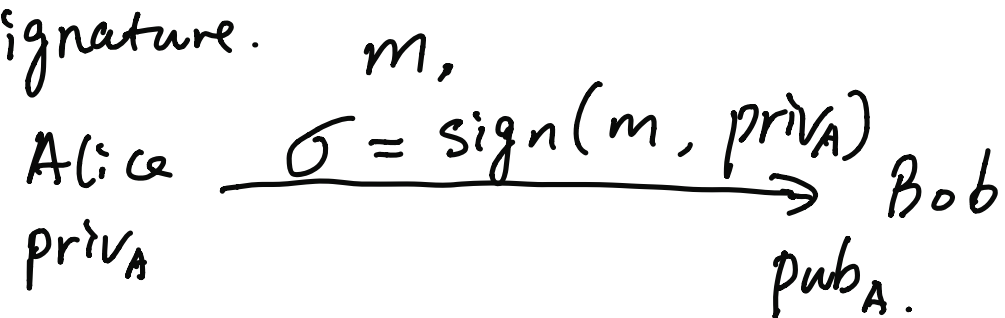
plaintext m



Key exchange.



Signature.



Bob: $\text{Verify}(\sigma, m)$
 pub_A

\neq true/false.

Euler's Theorem

Given $a \in \mathbb{Z}_n^* = \{1, \dots, n-1\}$

$$a^x \equiv a^{\underline{x \bmod \varphi(n)}} \pmod{n}.$$

$$\varphi(p) = p-1 \quad \varphi(10) = 4.$$

prime

1, 3, 7, 9.

$$a^5 \equiv a^{5 \bmod 4} = a \pmod{10}$$

$$a \equiv a^{1 \bmod \varphi(n)} \pmod{n}.$$

$$a^0 = 1 \equiv a^{0 \bmod \varphi(n)} \pmod{n}$$

$$a^4 \equiv 1 \pmod{10}$$

$P=7$ $\begin{matrix} x \\ a \end{matrix}$	1	2	3	4	5	6	7	$\pmod{7}$
1	1	1	1	1	1	1	1	
2	2	4	1	2	4	1	2	
3	2	2	6	4	5	1	3	

4	4	2	1	4	2	1	4
5	5	4	6	2	3	1	5
6	6	1	6	1	6	1	6

$$a^{p-1} = a^6 = 1 \pmod{7}$$

if p is prime: $\phi(p) = p-1$.

$$\phi(7) = 6$$

$$a^{p-1} \pmod{p} = 1.$$

Fermat's Theorem

RSA . Large primes. p, q (secret)

public $n = p \times q$.

choose e (public) relatively prime to $\phi(n)$

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

find mul. inverse d , $e \times d \equiv 1 \pmod{\phi(n)}$

public key is $\langle e, n \rangle$

private key $\langle \underline{d}, n \rangle$
secret

Enc: given m . $C = m^e \bmod n$

Dec: $\dots C$, $m = C^d \bmod n$

Correct:

$$\begin{aligned} C^d \bmod n &\equiv (m^e \bmod n)^d \bmod n \\ &\equiv (m)^{e \cdot d} \bmod n \\ &\equiv m^{1 \bmod \phi(n)} \bmod n \\ &\equiv m \bmod n = m \end{aligned}$$

$$m < n$$

Ex1. $p = 11$, $q = 7$. $n = 77$

$$\phi(n) = 10 \times 6 = \underline{60}$$

$$e = 37 \quad d = e^{-1} \bmod 60 \\ = \underline{13} \quad ed = 481.$$

Let $m = 15$

$$\begin{aligned} C &= m^e \bmod n = 15^{37} \bmod 77 \\ &= 71 \end{aligned}$$

$$\text{Dec: } C^d \bmod n = 71^{13} \bmod 77 = 15$$

Ex2. $p=3$. $q=11$. $n=33$

$$\phi(n) = 2 \times 10 = 20$$

$$e = 7. \quad d \cdot e \equiv 1 \pmod{20}$$

$$d = 3.$$

$$m^e = 5^7 \pmod{33} = 14.$$