ECE 471/571 Public key crypto (PKC)

plaintext m

Alice $\xrightarrow{C = E_{pub_B}(m)}$ Bob

pub_A, $priv_A$. $\qquad\qquad$ pub_B, pub_A. $\quad priv_B$

pub_B

public. $\qquad\qquad$ $Dec_{priv_B}(C) = m$

Key exchange.

Alice $\xrightarrow{E_{pub_B}(r)}$ Bob

nonce r $\quad \xleftarrow{DES_r(m)} \quad$ Dec r

Dec m

Signature. m,

Alice $\xrightarrow{\sigma = sign(m,\ priv_A)}$ Bob

$priv_A$ $\qquad\qquad$ pub_A.

Bob: $Verify_{pub_A}(\sigma, m) \stackrel{?}{=}$ true / false.

Euler's Theorem

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

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

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

1, 3, 7, 9.

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

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

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

$$a^4 \equiv 1 \bmod 10$$

mod 7

$p=7$ $a \backslash x$	1	2	3	4	5	6	7
1	1	1	1	1	1	1	1
2	2	4	1	2	4	1	2
3	3	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

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

if p is prime. $\varphi(p) = p-1.$ $\qquad \varphi(7) = 6$

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

$\boxed{\text{Fermat's Theorem}}$

RSA. Large primes. p, q. (secret)

public $n = p \times q$.

choose $\underline{e}$ (public) relatively prime to $\varphi(n)$

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

find mul inverse $\underline{d}$, $e \times d \equiv 1 \bmod \varphi(n)$

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

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

secret

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

Dec: .... c, $m = c^d \bmod n$

correct: $c^d \bmod n \equiv (m^e \bmod n)^d \bmod n$

$\equiv (m)^{e \cdot d} \bmod n$

$\equiv m^{1 \bmod \varphi(n)} \bmod n$

$\equiv m \bmod n = m$

$m < n$

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

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

$e = 37$ $d = e^{-1} \bmod 60$

$= \underline{13}$ $ed = 481$.

Let $m = 15$

$c = m^e \bmod n = 15^{37} \bmod 77$

$= 71$

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

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

$\varphi(n)=2\times10=20$

$e=7$. $d\times e\equiv 1 \bmod 20$

$d=3$.

$m^e=5^7 \bmod 33=14$.