RSA algorithm

keygen (1^n) - Choose 2 primes p, q.

Compute $n = pq$. $\phi(n) = (p-1)(q-1) =$ even

Choose e such that $GCD(e, \phi(n)) = 1$, &

$1 < e < \phi(n)$.

Compute $d = e^{-1} \bmod \phi(n)$

Public key $= (n, e)$

Private key $= (p, q, d)$

Note:

$\phi(n)$ = numbers which are less than n and are relatively prime to n.

~~$p, 2p, \ldots qp$~~

Encryption (M, n, e)

$$C = M^e \bmod n$$

Decryption (C, p, q, d)

$$M = C^d \bmod n$$

Correctness:

To prove RSA works, we have to show

$$dec(enc(M)) = M$$

or $C^d \bmod n = M$

or $M^{ed} \bmod n = M$

Case 1:

$$GCD(M, n) = 1$$

$\Rightarrow M \neq$ multiple of p or q

Using Euler's Theorem,

$$M^{\phi(n)} \equiv 1 \bmod n,$$

if $GCD(M, n) = 1$

It can be rewritten as

$$M^{\phi(n)} \bmod n = 1$$

If n is prime, $\phi(n) = n - 1$

and we have Fermat's theorem

$$M^{n-1} \bmod n = 1$$

$M^{ed} \bmod n = M$

or $M^{ed-1} \bmod n = 1$

or $M^{k\phi(n)} \bmod n = 1$ $\left[d = e^{-1} \bmod \phi(n) \Rightarrow \phi(n) \mid ed-1 \right]$

We know $(M^{\phi(n)})^k \bmod n = 1$,

So, $(M^{\phi(n)})^k \bmod n = 1$

Case 2: $GCD(M, n) \neq 1$

$M = p, 2p, 3p, \ldots qp$

$M = q, 2q, \ldots pq$

a) $M = ip$ (suppose)

$M^{q-1} \bmod q = 1$ [Fermat's Theorem]

$M^{(p-1)(q-1)} \bmod q = 1$

$M^{\phi(n)} - 1 = tq$

$M^{\phi(n)} = tq + 1$

$M^{\phi(n)} \cdot M = M + itpq$ [Multiply M on both sides]

$M^{ed-1} \cdot M = M + itn$

Taking modulo on both sides with n

$$M^{ed} \bmod n = M$$

b) If $M = j^q$, we could follow the same procedure as above

Chinese Remainder Theorem

Find x

$$x \bmod 3 = 2$$
$$x \bmod 5 = 3$$
$$x \bmod 7 = 2$$

According to Chinese Remainder theorem it is possible to solve for

$$x \equiv a_1 \bmod n_1$$
$$x \equiv a_2 \bmod n_2$$
$$\vdots$$
$$x \equiv a_K \bmod n_K$$

if $GCD(n_i, n_j) = 1$
and $1 \leq i, j \leq K$

Method:

$$N = n_1 n_2 \ldots n_K$$

$$N_1 = \frac{N}{n_1}, \quad N_i = \frac{N}{n_i}$$

$GCD(N_i, n_i) = 1$

$\therefore N_i^{-1} \bmod n_i$ exists

$$x = [a_1 N_1 (N_1^{-1} \bmod n_1) + \ldots + a_K N_K (N_K^{-1} \bmod n_K)] \bmod N$$

$$N = 3 \times 5 \times 7 = 105$$

$$N_1 = 35, \quad N_2 = 21, \quad N_3 = 15$$

$$x = [2 \times 35 \times (35^{-1} \bmod 3) + 3 \times 21 (21^{-1} \bmod 5) + 2 \times 15 (15^{-1} \bmod 7)] \bmod 105$$

$$= [2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1] \bmod 105$$

$$= 253 \bmod 105$$

$$x = 43$$

RSA decryption

Improving Chinese Remainder Theorem

Dec(C, d, p, q, n)

$$C^d \bmod p = Q_p$$

$$d = x(p-1) + d \bmod p-1$$

$$C^{x(p-1)+d \bmod (p-1)} \bmod p = (C^{p-1})^x \bmod p \cdot C^{d \bmod (p-1)} \bmod p$$

$$= C^{d \bmod (p-1)}$$

$$c^d \equiv O_p \bmod p \quad \text{where}$$

$$O_p = c^{d \bmod (p-1)} \bmod p$$

Similarly

$$c^d \equiv O_q \bmod q \quad \text{where}$$

$$O_q = c^{d \bmod (q-1)} \bmod q$$

Applying CRT,

$$n_1 = p \quad , \quad N_1 = q \qquad N = pq$$

$$n_2 = q \qquad N_2 = p$$

$$c^d = \left[\left(c^{d \bmod (p-1)} \bmod p \right) q \left(q^{-1} \bmod p \right) + \left(c^{d \bmod (q-1)} \bmod q \right) p \left(p^{-1} \bmod q \right) \right] \bmod pq$$

One way function

$$f : X \to Y$$

① f(x) can be computed in polynomial time.

RSA is a trapdoor one-way function. In RSA, it is easy to calculate forward as well as backward if trapdoor is given.

RSA hard problem

$$c = M^e \bmod n$$

Given c, e, n, finding M is a hard problem (takes exponential time)

Broadcasting

Suppose 3 people in a group are broadcasting with the same public key

$$c_1 = M^3 \bmod n_1$$

$$c_2 = M^3 \bmod n_2$$

$$c_3 = M^3 \bmod n_3$$

$$M^3 \equiv c_1 \bmod n_1$$

$$\vdots$$

$$M^3 \equiv c_3 \bmod n_3$$

Using CRT, we can compute

$$M^3, n_1, n_2, n_3$$

Note:

$$y = M^i \bmod n, \quad i \geq 3$$

Given y, i, n, it is hard to compute M.

But $M^3 < N_1, N_2, N_3$ (Rule of RSA),

$$M = y^{1/3}$$

Quadratic residue

$$x^2 \equiv a \bmod p$$

If a is quadratic residue mod p, the above equation is solvable.

If the above equation is not solvable, a is quadratic non-residue mod p.

$x^2 \equiv 1 \bmod 11$

$x = 1, 10$

$x^2 \equiv 2 \bmod 11$

(not solvable)

$x^2 = 3 \bmod 11$

$(x = 5, 6)$

Euler criteria

a is Quadratic residue mod p if

$a^{(p-1)/2} \bmod p = 1$

else a is Quadratic non residue mod p

Proof:

Suppose $x = a^{(p+1)/4} \bmod p$

$x^2 = a^{(p+1)/4 \bmod p} =$

To find x in $x^2 \equiv a \bmod p$

check whether $a^{(p-1)/2} \bmod p = 1$

and $p \equiv 3 \bmod 4$, then

$x \equiv a^{(p+1)/4} \bmod p$

Advanced Cryptography

Security Definitions

1. Given Cipher Text C, it is hard to find private key. This is however, not a good definition of Security.

2. Given cipher Text, it should be hard to find corresponding plain Text. However, adversary may know some part of plain text.

3. Given Cipher Text; it should be hard to find any part of the corresponding plain text (or) Cipher Text should not reveal anything about plain text.

This is the definition of Perfect Security.

In terms of probability,

$$P(M = m) = P(M = m / C = c)$$

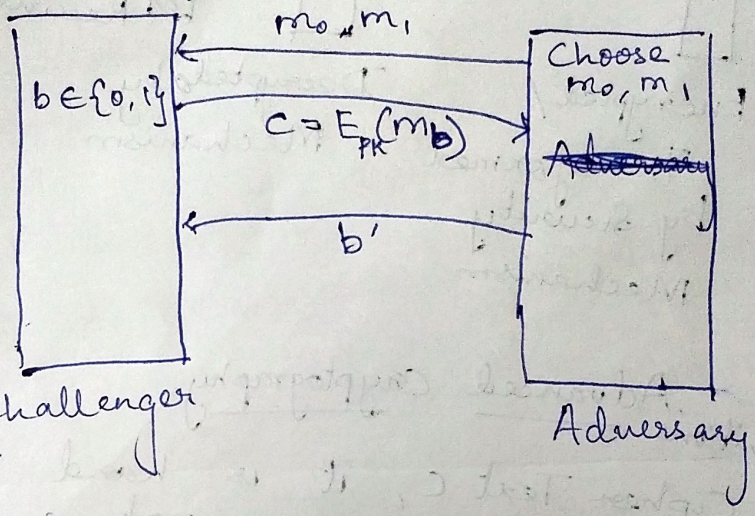
4. Encryption scheme is perfectly secure if and only if

$$P(M = m_0 / C = c_0) = P(M = m_1 / C = c_1)$$

$$= \text{const}$$

M : message space

5. Perfect security is equivalent to the game played between Adversary and Challenger.



$$Adv_{A,\pi}(n) = P[b == b'] - 1/2$$

Scheme is perfectly secure

if $\boxed{Adv_{A,\pi}(n) = 0}$

$\therefore$ IND $\approx$ IND - CPA

Note:

Perfectly secure schemes are not practical.

In practical cases, it is enough if

$$Adv_{A,\pi}(n) \leq 1/2^{80}$$ (less than negligible)

One time key

$$C = M \oplus K$$

K should be changed every time.

Result:

Perfectly secure scheme is not practical.

A scheme is secure (semantically) if and only if $Adv_{A,\pi}^{(n)} \leq neg(n)$.

We have different attacks

Known plain text : $M \to C$

Chosen plain text : choice $M \to C$

Known cipher text attack : $C \to m$

} not useful for public key cryptography

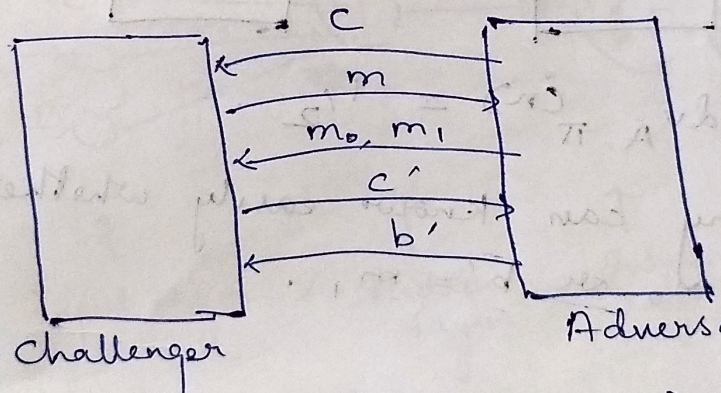
Chosen cipher text : Choice $C \to m$

Chosen cipher text 2 : ~~Choice~~ Choice $C \to m$ (adaptively)

} useful for public key

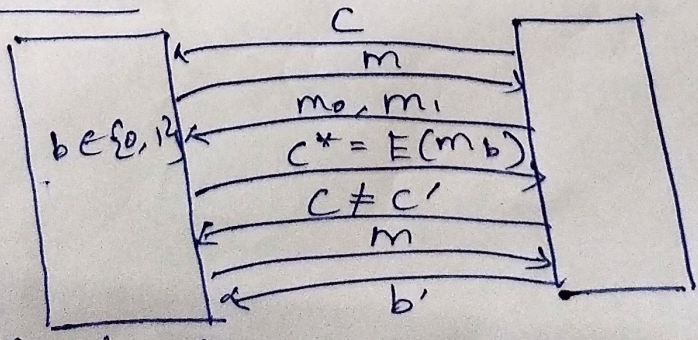
~~Chosen cipher text~~

IND-CCA



If $Adv_{A,\pi}^{(n)} \leq neg(n)$, the above scheme is IND-CCA secure

IND-CCA2



If $Adv_{A,\pi}^{(n)} \leq neg(n)$, the above scheme IND-CCA2 Secure

Deterministic Encryption scheme

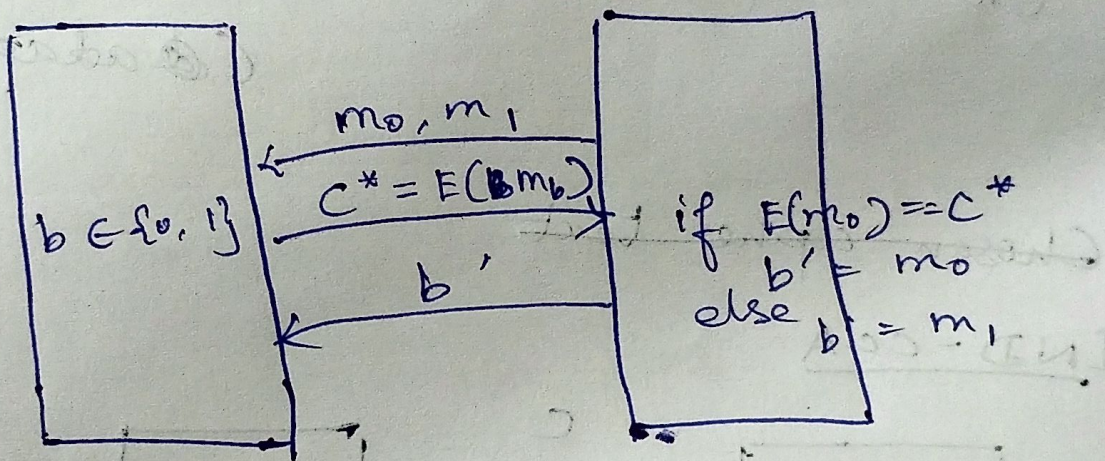
- A plaintext always has the same corresponding cipher text.

Deterministic schemes are not ~~IND~~ secure semantically.

Theorem :

Text RSA is not IND-CPA secure (semantically)

~~Public key cryptosystem is not IND-CPA~~



$$Adv_{A,\pi}^{(n)} = 1/2$$

Adversary can know easily whether $b' = m_0$ or $b' = m_1$.

Advanced Cryptography

RSA: CCA secure (to prove)

His choice: $c \to P$

Objective: Decrypt $c^* \to m^*$

$$c^* = m^{*e} \bmod n$$

Adversary choose random no. r

$$c = r^e c^* = (rm^*)^e \bmod n$$

Ask plaintext for c,

answer $m = rm^*$

We know r, m

$$\boxed{m^* = r^{-1} m}$$

∴ Textbook RSA is not CCA secure.

Malleability

PKE scheme is malleable if adversary can transfer c^* to c' such that

$$d(c') = f(d(c^*))$$

Check whether RSA is malleable

Adversary knows c^*

Choose random no. r

$$c = r^e c^* = (m^* r)^e \bmod n$$

$$d(c) = f(d(c^*))$$

$$d(c) = m^* r$$

$$\boxed{d(c) = d(c^*).r}$$

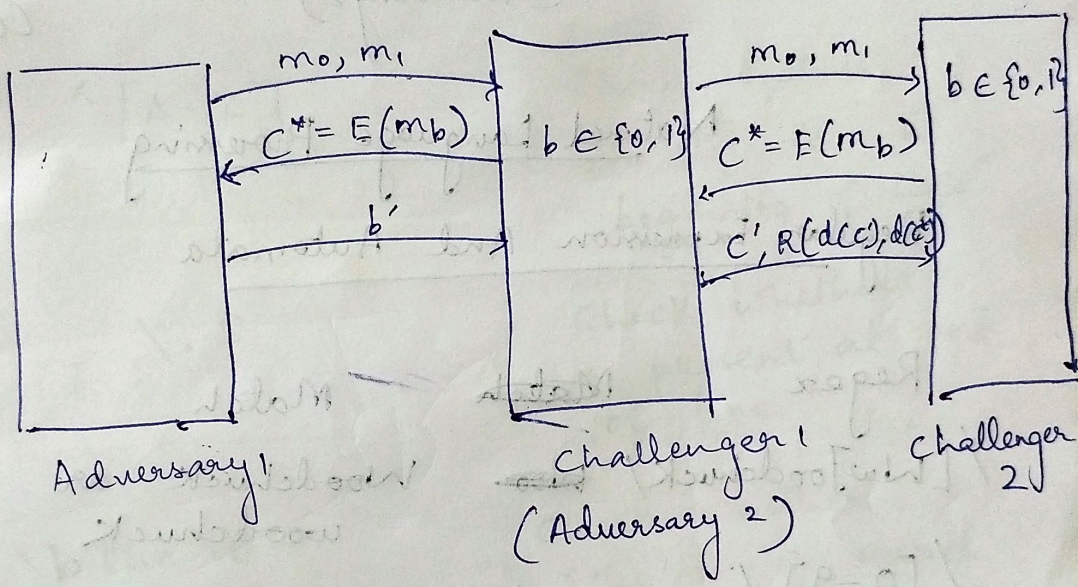
Theorem

PKE is secure in NM-CPA, then PKE is secure in IND-CPA.

This can be rewritten as:

Adversary can break PKE in IND-CPA $\Rightarrow$ Adversary can break PKE in NM-CPA with (non negligible probability in polynomial time).

Game definition



Suppose

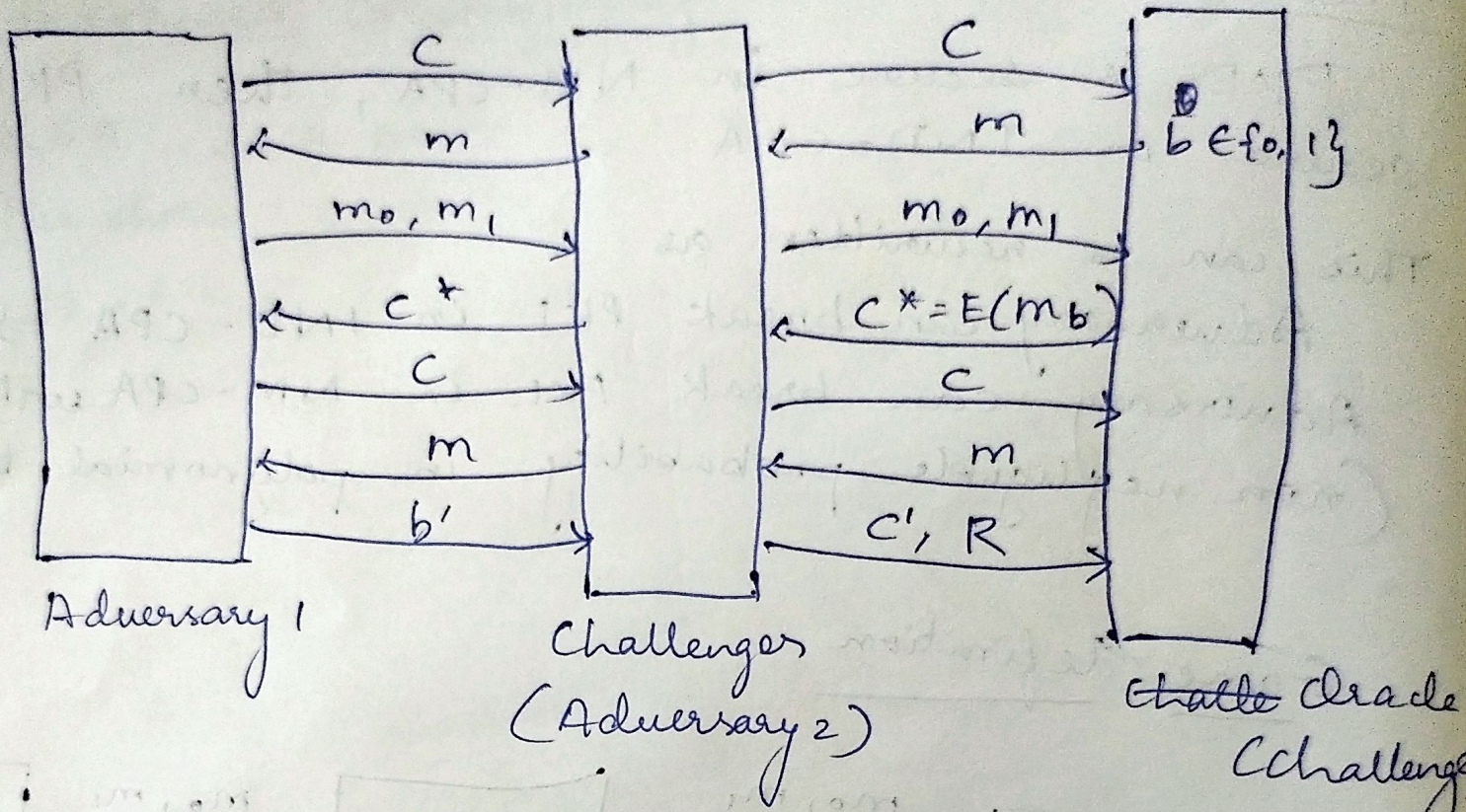
$$E(m') = C'$$

$$E(m_b^* + 1) = C'$$

$$m' = m_b^* + 1$$

Theorem

PKE is secure NM-CCA2, then PKE is secure in IND-CCA2.

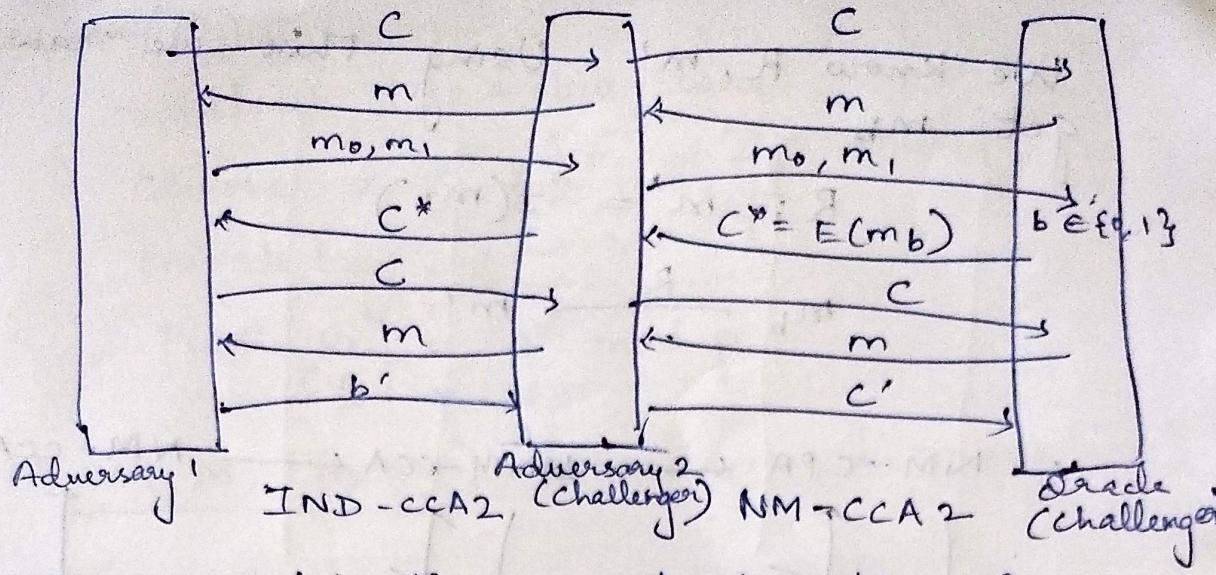

c
m
m0, m1
c*
c
m
b'
c
m
b ∈ {0, 1}
m0, m1
c* = E(mb)
c
m
c', R
Adversary 1
Challenger
(Adversary 2)
Oracle
Challenger

Advanced Cryptography

Theorem: IND Scheme is secure in NM = CCA2 if and only if scheme is secure in IND-CCA2

NM-CCA2 ⟶ IND-CCA2

If adversary can break scheme in IND-CCA2 then another adversary can break scheme in NM-CCA2.



IND-CCA2 NM-CCA2

Assume b' is the correct decryption of c^*.

~~$c' = E(m_{b'})$~~

$$c' = E(f(m_{b^*}))$$

~~Let $f(m_b) = m$~~

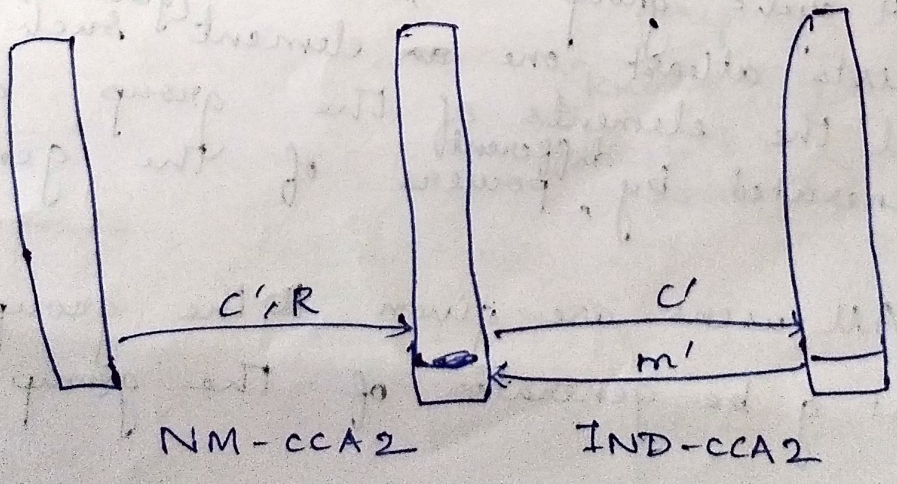
Let $f(m_{b^*}) = m_{b^*} + 1$

$$c' = E(m_{b^*} + 1)$$

$$R : d(c') = d(c^*) + 1$$

The inverse is also true:

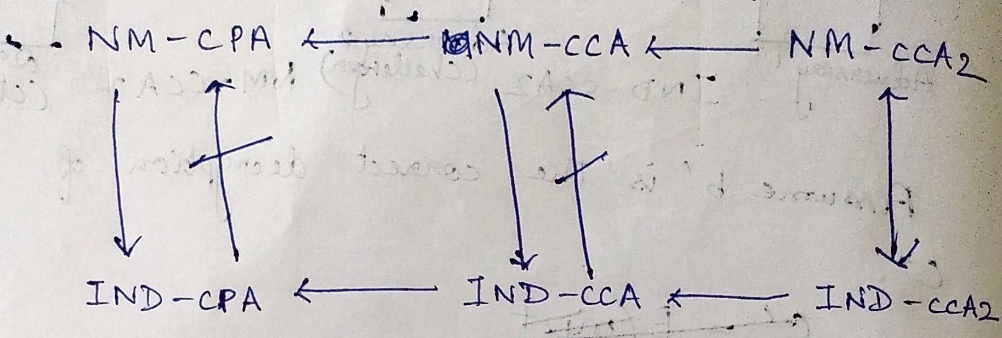
If adversary can break scheme in NM-CCA2, then another adversary can break scheme in IND-CCA2.



We know R, m'. Using this we can get m_b

$$R : m' = f(m_b)$$

$$m_b \xrightarrow{R} m'$$



Adaptivity

$$C_i = f(M_{i-1}, C_{i-1})$$

IND-CCA2, NM-CCA2 are adaptive ciphers.

Elgamal Encryption

Choose a prime number p such that the group $(Z_p^*, *)$ is a cyclic group

$$Z_p = \{1, 2, \ldots, p-1\}$$

A cyclic group is a group in which there exists atleast one element (generator) such that all the elements of the group can be generated by different powers of the generator.

All users are given the group Z_p. Let g be generator of the group

Key gen (1^n):

- atleast 1024 bits long

Choose $x \in [2, p-2]$.

Private key $= x$

Public Key, $(y) = g^x \bmod p$.

Enc (M, $PB_R = y$) (Randomized encryption)

Choose $k \in [2, p-2]$ randomly

~~$c_1 = g^k$, $c_2 =$ [illegible]~~

$c_1 = g^k$

$c_2 = M y^k$

Dec (c_1, c_2, x):

$M = c_2 (c_1^x)^{-1}$

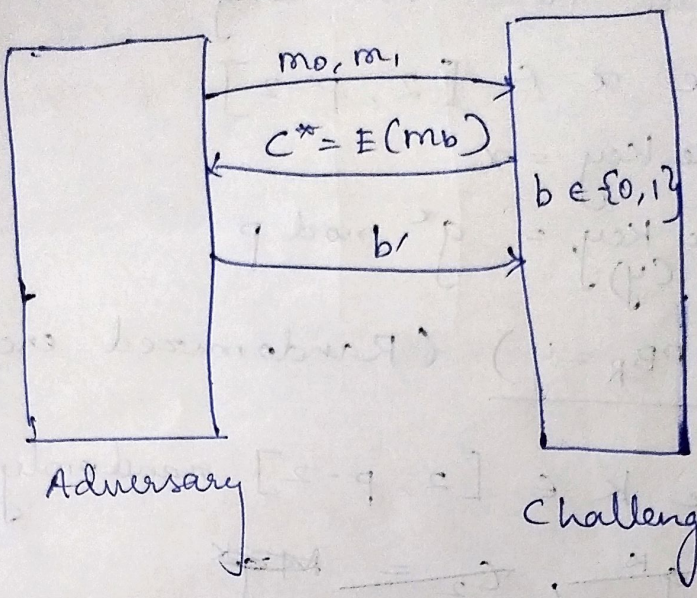
Proof

$y = g^x \Rightarrow \boxed{y^k = g^{xk} = (g^x)^k = (g^k)^x}$

Sender's perspective (Knows k, y) (doesn't know x)

Receiver's perspective (Knows x, y) (doesn't know k)

Elgammal is not IND-CPA secure



$$Adv_{A,\Pi}^{(n)} = Prob(b == b') - 1/2$$

If $Adv_{A,\pi}^{(n)}$ is non-negligible, the scheme is said to be broken

We have to prove that g is ~~Quadratic~~ Non-residue mod p.

We should show, There doesn't exist x such that

$$x^2 \equiv g \bmod p$$

If $g^{(p-1)/2} \bmod p = -1$, g is quadratic non-residue mod p.

Since g is generator of Z_p,

$$g^{p-1} \bmod p = -1$$

$(p-1)$ is the order of the g ~~group~~ p.

Therefore, $g^{p-1} \bmod p = 1$

$g^{(p-1)/2} \bmod p = 1$ or -1

If $g^{(p-1)/2} \bmod p = 1$, order of $g = \frac{(p-1)}{2}$

which contradicts the fact that order of $g = (p-1)$.

Therefore, $g^{(p-1)/2} \bmod p = -1$

$c_1 = g^k$, $c_2 = my^k$

Case 1:

y is Quadratic residue mod p, then y^k is also quadratic residue mod p.

$c_2 \longleftrightarrow m$

If m is QR mod p, c_2 is also QR mod p.

Adversary only has to check if m_b = QR(b), m_{1-b} = QNR(b) original message is m_b.

Case 2:

y is Quadratic non residue mod p

$c_1 = g^k$

a) c_1 is QR $\Rightarrow$ k is even

$c_2 \longleftrightarrow m$ [y^k is 1]

b) c_1 is QNR $\Rightarrow$ k is odd

$c_2 \longleftrightarrow -m$ [y^k is -1]

∴ In this case if c_2 is QR, m is QNR

or if c_2 is QNR, m is QR

Modified Elgammal

In this modification, g is chosen such that g is Quadratic residue mod p.

Schnorr group

$$Z_7 = \{1, 2, 3, 4, 5, 6\}$$

$$= \{3, 3^2, 3^3, 3^4, 3^5, 3^6\} \quad g = 3$$

We create a new cyclic subgroup from Z_7 called G_1

$$G_1 = \{3^2, 3^4, 3^6\}$$

$$= \{2, 4, 1\}$$

This group G_1 is called Schnorr Group.

Schnorr Group (Definition)

Choose primes p, q such that q divides (p-1). Cyclic subgroup of order q is called Schnorr group.

Assume we have a cyclic group Z_p with generator h.

$$Z_p = \{h, h^2, \ldots h^{p-1}\}$$

Let $p - 1 = 2q$

Let the new generator, $g = h^2$

The new group G_1 with generator g has q elements.

Regardless of whether h is QR mod p or QNR mod p, g will be QR mod p.

M is also QR mod p;

C is also QR mod p

Key gen (1^n): Choose $x \in \{G - \{1\}$

$PR = x$

$PB = g^x$

Proove that

Elgammal is not CCA secure

$c_1^* = g^k$, $c_2^* = my^k$

Ask plain text for a suitable c' that will reveal c^*.

$c' = (c_1', c_2')$

Choose

$c_1' = g^k$, $c_2' = r\, c_2^*$

~~Using this, we can find~~

Prove that

$dec(c_1', c_2') = m'r$

Advanced Cryptography

Field

Field set F along with 2 operations $\oplus$ and $\circledast$ is a field if it satisfies the following properties:

(i) $\langle F, \oplus \rangle$ is a commutative group

- closure property.
  $\forall a, b \in F \quad a \oplus b \in F$
- Associativity
- Identity. $\exists e \in F$ such that
  $a \oplus e = e \oplus a$
- Inverse. Every element must have additive inverse
  $a \oplus a^{-1} = e$
- Commutativity
  $\forall a, b \in F,$
  $a \oplus b = b \oplus a$

(ii) $\langle F, \circledast \rangle$ should have the following properties

- Closure
- Associativity
- Identity. $\exists e' \in F$ such that
  $a \circledast e' = a$
- Except additive identity e, all the other elements should have inverse with respect to $\circledast$

- Commutativity
- Distributivity of $\circledast$ over $\oplus$

$$a \circledast (b + c) = (a \circledast b) \oplus (a \circledast c)$$

$Z_p = \{0, 1, 2, \ldots, p-1\}$, $+ \bmod p$, $\times \bmod p$

$\langle Z_p, +, \times \rangle$ is a field.

$\langle R, +, \times \rangle$ is a field

In cryptography, fields consisting of prime number of elements is used.

~~Field of size 2^n~~

Field (2^n)

~~$Z_2 = \{0, 1\}$, $+ \bmod 2$, $\times \bmod 2$~~

Prime polynomial is used, over the field R

Note:
A prime polynomial is a polynomial which cannot ~~over~~ be factorized.

$x^2 + 1$ is a prime polynomial over the field R only. In the field C, x^2+1 can be factorized as $(x - i)(x + i)$.

So, x^2+1 is not a prime polynomial over the field C.

$F = \langle \{ a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \}, +$ mod pp of degree n, $\times$ mod pp of degree $n \rangle$

$a_i \in Z_2$

$|F| = 2^n$

$\langle F, +$ mod pp of degree $n \rangle$

1) Closure example

$$1 + x + x^2$$
$$x + x^2$$
$$\overline{1 + (1+1)x + (1+1)x^2}$$

Here $1+1 \neq 2$ as we should perform operations with respect to Z_2.

$1 + 1 = 0$

2) Additive inverse

The same polynomial is its own additive inverse

3) Additive identity

0 is the additive identity

Theorem: Given x, y, $\exists$ a, b such that $ax + by = GCD(x, y)$

Advanced Cryptography

$28^{-1} \bmod 75$

$x = 75, \quad y = 28$

Find a, b s.t $ax + by = GCD(75, 28) = 1$

	q		
75		1	0
28	2	0	1
19	1	1	-2
9	2	-1	3
1		3	-8
0			

→ Inverse of 28 mod 75

$-8 \bmod 75 = (67 - 75) \bmod 75 = 67$

$3 \times 75 + (-8) 28 = 1$

or $[3 \times 75 + 67 \times 28 \equiv 1] \bmod 75$

Note:

$[ax + by = 1] \bmod x$

$[axy^{-1} + byy^{-1} = y^{-1}] \bmod x$

$b = y^{-1} \bmod x$

~~Hence we are~~

Field (2^3)

$a_2 x^2 + a_1 x + a_0 \qquad a_i \in GF(2)$

Note:

$\mathbb{Z}_2$ is also called Galois field (2).

Consider 2 elements belonging to Field(2^3)

x^2+x, x^2+x+1

Find a, b s.t

$a(x^2+x) + b(x^2+x+1) = GCD(x^2+x, x^2+x+1)$

	a		
x^2+x		1	0
x^2+x+1	1	0	1
1		1	−1

$a = 1$, $b = -1 \bmod 2 = 1$

$$
\begin{array}{r|l}
 & 1 \\
\hline
x^2+x+1 & x^2+x \\
 & x^2+x+1 \\
\hline
 & 1 \\
\hline
\end{array}
$$

Instead of $x^2+x - x^2-x-1$, we can change it to x^2+x+x^2+x+1, because -1 doesn't belong to Z_2, but

$-1 \equiv 1 \bmod 2$

$-x^2-x-1 \equiv x^2+x+1$ (w.r.t to Z_2)

Problem:

$a(x^3+x) + b(x^2+x+1) = GCD(x^3+x, x^2+x+1)$

	q		
x^3+x		1	0
x^2+x+1	$x+1$	0	1
$x+1$	x	1	$x+1$
1		x	$1+x+x^2$
0			

$$\begin{array}{r|l} & x+1 \\ x^2+x+1 & x^3+x \\ & -x^3+x^2+x \\ \hline & 0+x^2+0 \\ & -x^2+x+1 \\ \hline & 0+x+1 \end{array}$$

$$\begin{array}{r|l} & x \\ x+1 & x^2+x+1 \\ & -x^2+x \\ \hline & 0+1 \end{array}$$

$a = x$

$b = 1+x+x^2$

$(x^2+x+1)^{-1} \bmod (x^3+x) = x^2+x+1$

$(x^3+x)^{-1} \bmod (x^2+x+1) = x$

Field (p^n)

- also called extended field

$F = a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$

$a_i \in Z_p$ (field)

Field (p^n) = $\langle F, +$ mod pp of deg n (in field Z_p), $\times$ mod pp of deg n (in field Z_p)$\rangle$

To prove that Field (p^n) is a valid field

$\langle F, + \rangle$

- closure
- associative
- identity (Zero polynomial)
- Inverse $= (p - c) \bmod p$
- commutative

$\langle F, \times \rangle$

- Using extended Euclidean algorithm, we can prove that inverse exists for all elements in Z_p except for 0.

E.g Field(3^2)

$F = \{ a_1 x + a_0 \}$ $\quad a_i \in Z_3 = \{0, 1, 2\}$

+ mod pp of deg 2

× mod pp of deg 2

Field(5^4)

$F = \{ a_3 x^3 + a_2 x^2 + a_1 x + a_0 \}$

$a_i \in$ ~~$\{0, 1, 2, 3\}$~~,

Z_5 (field)

+ mod pp of degree 4,

× mod pp of degree 4

Advanced Cryptography

Field (5^3)

$F = \{ a_2 x^2 + a_1 x + a_0 \}$

Take 2 elements of Field (5^3),

$p(x) = 4x^2 + 3x + 1$

$q(x) = 3x + 4$

Use extended euclidean algorithm to find a and b s.t

$a\,p(x) + b\,q(x) = GCD(p(x), q(x))$

$4x^2+3x+1$		1	0
$3x+4$	$3x+2$	0	1
3	$x+3$	1	$2x+3$
0			

$$1-(x+3)(2x+3) = 1-2x^2-9x-9$$
$$= 10-2x^2-9x-8$$
$$= 3x^2+x+2$$

a	$4x+3$
b	$3x^2+x+2$

Inverse doesn't exist as GCD = 1

Field (5^4)

$F = \{ a_3x^3 + a_2x^2 + a_1x^1 + a_0 \}$

$p = 5$, $n = 4$

$p(x) = 3x^3 + 4x^2 + 4x + 1$

$q(x) = 2x^2 + 4$

Find a, b s.t

$$a\,p(x) + b\,q(x) = GCD(p(x), q(x))$$

$3x^3+4x^2+4x+1$		1	0
$2x^2+4$	$4x+2$	0	1
$3x+3$	$4x+1$	1	$x+3$
1		$x+4$	x^2+3x+3
0			

$$4x+2$$
$$2x^2+4 \;\big|\; 3x^3+4x^2+4x+1$$
$$3x^3+0x^2+x$$
$$0+4x^2+3x+1$$
$$4x^2+0+3$$
$$0+3x+3$$

$$4x+1$$
$$3x+3 \;\big|\; 2x^2+4$$
$$2x^2+3x$$
$$0+3x+4$$
$$3x+3$$
$$1$$

$$= 1 - (Ax+1)(x+3)$$

$$= 1 + x^2 + 2x + 2$$

$$= x^2 + 2x + 3$$

$$a = x + 1$$
$$b = x^2 + 2x + 3$$

Note:

$q(x)^{-1} \bmod p(x) = b$

$p(x)^{-1} \bmod q(x) = a$

Characteristic number

Number of times multiplicative identity has to be added to get additive identity

Field (Z_2)

Characteristic number = 2

Field (Z_5)

Char. number = 5

For Field (Z_p), char. number = p

For Field (2^n), char. number = 2

For Field (p^n), char. number = p

For Field (R), where R is field of real numbers, char. number = 0

Eliptic curve (cubic equation)

Note:

	Key Size
Eliptic curve	256
Elgammal	3072
RSA	3072
AES	128

Symmetric key encryption is more efficient than Asymmetric key encryption because of smaller key size.

Eliptic curve (cubic equation)

For characteristic number $\neq 2$

$$y^2 = x^3 + ax + b$$

The graph of above equation is symmetric about x-axis.

Network Security

MAC (Message Authentication code)

- A many-to-one mapping
- fixed length code

$$MAC = C(K, M)$$ [Symmetric key encryption]

K - Encryption key

M - Message

- It is a cryptographic checksum / tag

Advanced cryptography

Cryptographic hash functions

SHA 512

$$H: \{0,1\}^{+} \longrightarrow \{0,1\}^{512}$$

(i) One way function

Given y, it is hard to find x such that $H(x) = y$. It takes $O(2^{512})$

(ii) Secondary Image Resistant Property

Given x_1, it is hard to find x_2 such that $H(x_1) = H(x_2)$

(iii) Collision

Find x_1, x_2 such that

$$H(x_1) = H(x_2)$$

Birthday Paradom

How many person should be there in room so that atleast two person will have same birthday with probability $1/2$.

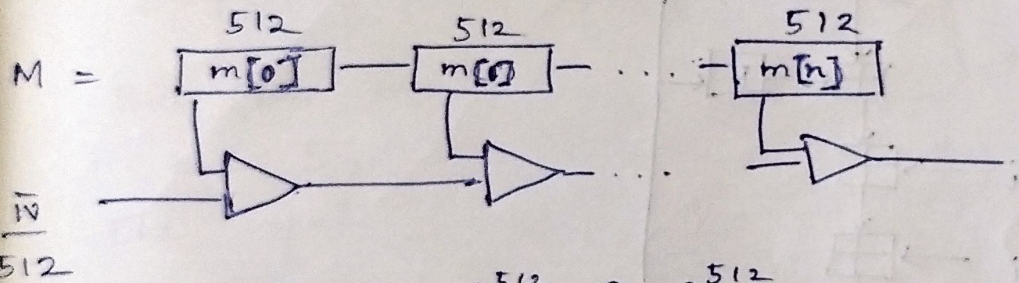
There should be atleast $(365)^{1/2} \approx 23$

Similarly, to find 2 numbers x_1, x_2 such that ~~time complexity~~ $hash(x_1) = hash(x_2)$ with probability $1/2$,

time complexity $= O(2^{512})^{1/2}$

$= O(2^{256})$

Merkel - Damgaard (MD5)



$h : \{0,1\}^{512} \times \{0,1\}^{512} \longrightarrow \{0,1\}^{512}$

$H : \{0,1\}^{*} \longrightarrow \{0,1\}^{512}$

Theorem

If h is collision resistant then H is also collision resistant.

Digital signature

- Encrypt with private key
- Decrypt with public key and compare with original message.
- Digital signature must depend on the original message to prevent message from being tampered with.

Digital signature ensures the following

* Message Authentication
* Message Integration

Advanced Cryptography

Signature Schemes

1. Key Generation $(1^n) \longrightarrow PR, PK$
2. $Sig(m, PR) \longrightarrow s$
3. Verification $(m, s, PB) \longrightarrow$ accept / reject

Different types of forgeries

1. Existential Forgery (not dangerous)

   $m \longrightarrow s$

   (may not useful for attacker as attacker doesn't choose m).

2. Selected Forgery

   $m \longrightarrow s$

   (chosen by attacker)

Types of attackers

1. Normal attackers

   (don't know the signature)

2. Known Message attackers

   Attacker knows s for a particular m. He tries to find s for his own message m^*.

3. Chosen Message attackers

   Attacker knows signature (s) for his choice of m.

Security requirement

"Chosen Message attacker ~~should~~ can not existential forgery".

RSA

① PR : d, PB = e, n

② sig(m, d) $s = m^d \bmod n$

③ verify (m, s, e) $s^e \bmod n = m'$

if (m' == m)
accept
else
reject

$sig(m, m_2) = (m_1 m_2)^d \bmod n = (m_1^d \bmod n \; m_2^d \bmod n) \bmod n$

$= sig(m_1) \cdot sig(m_2)$

CMA adversary can make selective forgery.
To find signature of m, he can factorize m into m_1 and m_2.

CMA adversary can get signature for m_1 and m_2 and calculate sig(m) as,

$sig(m) = sig(m, m_2) = sig(m_1) \cdot sig(m_2)$

Problem

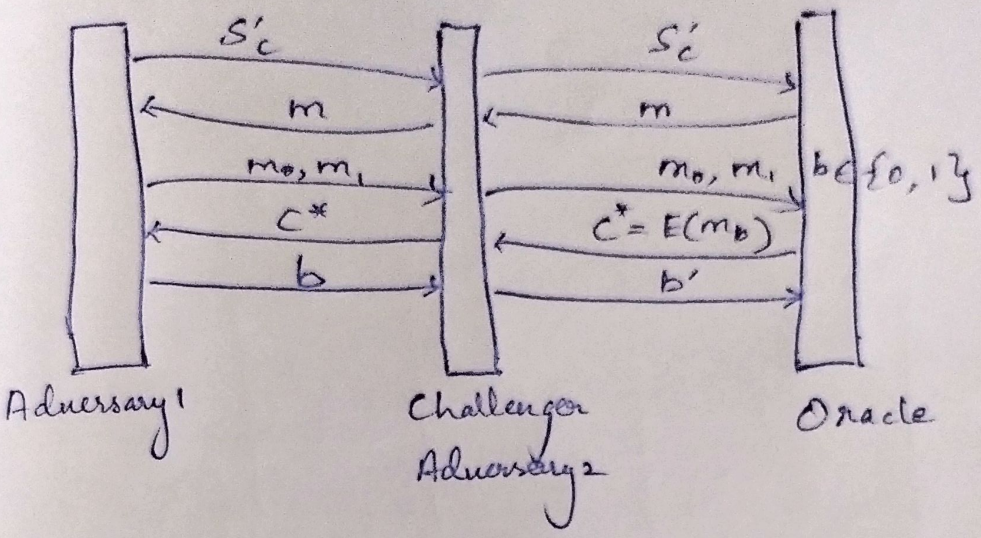
Let S(E, D) is IND-CCA secure. Prove or disprove that S'(E', D') is IND-CCA secure.

$E'(m) = E(m \oplus 1^{128})$

$D'(c) = D(c) \oplus 1^{128}$

By contrapositive,

If adversary can break scheme $S'(E', D')$ then there exist another adversary who can break scheme $S(E, D)$.

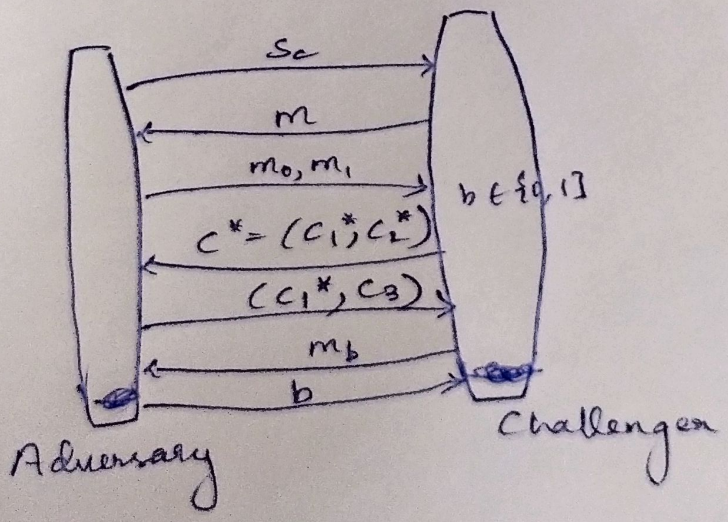


Problem

$E'(m) = (E(m), c_2)$

$D'(c_1, c_2) = D(c_1)$.

Show that the above scheme is not IND-CCA2 secure



Note:

To prevent $sig(m_1, m_2) = sig(m_1)\, sig(m_2)$

~~Calculate~~ apply padding to m

then ~~sign~~ we have $M = m \,||\, padding$

$S = M^d \bmod n$