11/8/22

Advanced Cryptography

Symmetic Cryptosystem (Before 1976)

(Pirati)

Pre-requisite - common key

Objective: ① Confidential Menage → done by AES

↳ 2 way of doing.

ⓐ Stream cipher - AES

ⓑ Block cipher - Salsa

② Authentication

MAC → Msg authentication code.

→ It is more efficient than asymmetic.

→ 95% public key

5% Pirati key.

Public key cryptography:-

1976 - Diffie Hellman gave idea of public key cryptography (Asymmetic).

→ Both mes will have 2 keys.

① Pirati key

② Public key.

Encryp:- Both keys.

Decryp:- Both key but decryp key has to be different from encryption key.

$Enc(M, PB_R) \rightarrow$ Ciphertext

$Dec(C, PR_R) \rightarrow M$

objective of Public key :-

① Confidentiality — RSA
\ Elgamal
\ ECC

② Authentication — (Digital signature)
RSA schnorr signature

③ → Hash function.

③ Blockchain 1.0 (Cryptocurrency)
Bitcoin
Blockchain 2.0 (Ethereum)
smart contract.

④ Zero knowledge Proof :-
↳ (I have ... and I want to convince u that I have secret without revealing secret.)

⑤ Multi-party computation (MPC)
2-party computation (2PC) : Yao
(Mukesh) (Anil Ambani)
fog)
→ without believing their wealth to each other we need to know who is richest.

1978 – RSA Algorithm (Rivert, Shamir, Adleman)

Key Gen (1^n) : 1024 bit
. less than 2^{1024}

→ choose 2 primes P, q of size 512 bit

→ compute $n = Pq$ ($n \rightarrow$ 1024 bit)

→ $\phi(n)$: No. of integers less than 'n' and relatively prime to n.

Eg:-

$\phi(20)$: 1, 3, 7, 9, 11, 13, 17, 19
$= 8$

$n = P_1^{r_1} P_2^{r_2} \dots P_i^{r_i}$

where $P_1, P_2 \dots P_i \rightarrow$ Prime

Eulers quotient

$\phi(n) = (P_1^{r_1} - P_1^{r_1-1}) \dots P_i^{r_i} - P_i^{r_i-1}$

$20 = 2^2 \cdot 5^1$

$\phi(20) = (2^2 - 2^1)(5^1 - 5^0)$
$= (4-2)(5-1)$
$= (2)(4) = 8$

12/08/2022

RSA Algorithm :- (Asymmetric (2 keys) cryptographic

KeyGen:

① choose two primes P, q

② compute $n = pq$ (key length)

$\phi(n) = (p-1)(q-1) = \text{even}$

③ choose e (public key) such that

$GCD(e, \phi(n)) = 1$ & $1 < e < \phi(n)$

④ compute $d = e^{-1} \bmod \phi(n)$

⑤ Public key = (n, e)

Private key = (P, q, d)

Enc $(m, n, e) \rightarrow c$

$c = m^e \bmod n$

Dec $(c, P, q, d) \rightarrow m$

Not using this pq :. it use pq if it is fast in CRT

compute $m = c^d \bmod n$

$\phi(n)$ → No. which r not multiple of P & q

:. P, q → Prime

use formula for $\phi(n)$

$P, 2P \ldots qP = q$

$q, 2q \ldots Pq = P$

$Pq - (P+q-1)$ → No. of numbers which r multiple of prime two

Correctness :-

dec (enc(m)) = m

$c^d \bmod n = m$

$\boxed{m^{ed} \bmod n = m}$ → Prove this

case 1 :- $GCD(m, n) = 1$

Euler's theorem :-

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

→ m can be not multiple of P or q

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

DOMS | Page No. | Date / /

divides n

$m^{\phi(n)} - 1$

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

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

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

$m^{ed-1} \bmod n = 1 \quad -①$

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

$\phi(n)$ / $ed-1$ $\Rightarrow$ $ed-1 = k\phi(n)$ ↓ put in ①

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

Message space
convert m into no.
whose range = $\{0, n-1\}$

Ciphertxt space
$\{0, n-1\}$.

n is prime.

$m^{n-1} \bmod n = 1$
Fermat's thm.

$a^{x-1} \Rightarrow a^x \cdot a^{-1}$

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

$m = P, 2P, 3P \ldots qP \quad (q-1)P$
$m = q, 2q, 3q \ldots Pq \quad (P-1)q$

ⓐ $m = iP$

$m^{q-1} \bmod q = 1 \Rightarrow \frac{q}{m^{q-1}-1}$

$m^{(P-1)(q-1)} \bmod q = 1$

$\Rightarrow m^{\phi(n)} - 1 = tq \Rightarrow \frac{q}{m^{(P-1)(q-1)}-1}$

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

Multiply m on both sides

$m^{\phi(n)} m = m + itPq$

$\phi(n) = ed - 1$

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

$m^{ed} = m + itn$

$\therefore$ mod n, on both sides

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

(b) $m = jq$

Chinese Remainder theorem:

① Find x:

$x \bmod 3 = 2$

$x \bmod 5 = 3$

$x \bmod 7 = 2$.

Soln:

$x \equiv 2 \bmod 3$

$x \equiv 3 \bmod 5$

$x \equiv 2 \bmod 7$

$x \equiv a_1 \bmod n_1$

$x \equiv a_2 \bmod n_2$

(*) $x \equiv a_3 \bmod n_3$ $\quad GCD(n_i, n_j) = 1$

$\vdots$

$x \equiv a_k \bmod n_k$ $\quad 1 \le i, j \le k$.

Method: $N = n_1 \cdot n_2 \cdots n_k$

$N_1 = \frac{N}{n_1}$; $N_i = \frac{N}{n_i}$

$GCD(N_i, n_i) = 1$

$N_i^{-1} \bmod n_i$ exist

$$x = [a_1 N_1 (N_1^{-1} \bmod n_1) + \dots + a_k N_k (N_k^{-1} \bmod n_k)] \bmod N$$

$2^{-1} \bmod 3 = 2$ $\quad 1-3 = -2$

$2^{-1} \bmod 5 = 3$ $\quad 3-5 = -2$

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

$N_1 = 35 = \frac{105}{3}$ $\quad N_2 = 21 = \frac{105}{5}$ $\quad N_3 = 15$ $\quad \frac{105}{7}$ (15)

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

$x_1 * x_2 \bmod n = [(x_1 \bmod n) * (x_2 \bmod n)] \bmod n$

$(* +, -, \times, \div)$

$35^{-1} \bmod 3 = (35 \bmod 3)^{-1} \bmod 3$

$= 2^{-1} \bmod 3 = 2.$

$x = (2 \cdot 35 \cdot (2) + 3 \cdot 21 \cdot (1) + 2 \cdot 15 \cdot (1)) \bmod 105$

$N_1 N_1^{-1} \bmod n_1 \equiv 1$

$35 * N_1^{-1} \equiv 1 \bmod 3$

$\frac{35 * 1 \% 3 = 5}{3}$ $\quad \boxed{N_1^{-1} = 2}$

$35 * 2 \% 3 =$

$70 \% 3 = 1.$

$N_2 N_2^{-1} \bmod n_2 \equiv 1$

$21 \cdot N_2^{-1} \bmod 5 \equiv 1$

$N_2^{-1} = 1$

$N_3 N_3^{-1} \bmod n_3 = 1$

$15 \cdot N_3^{-1} \bmod 7 = 1$

$N_3^{-1} = 1$

$x = [140 + 63 + 30] \bmod 105$

$= 233 \bmod 105$

$\boxed{x = 23}$

from video

DOMS | Page No. | Date / /

Extended Euclidean Algorithm

→ Multiplicative inverse is found by Extended Euclidean algorithm.

① Multiplicative inverse of 3 mod 5 = 2

Q	A	B	R	T_1	T_2	T	$T = T_1 - T_2$
	A ⅞ B						
1	5	3	2	0	1	-1	$T_1 \rightarrow$ M.I
1	3	2	1	1	-1	2	$1-(-1)(1)$ $1+1=2$
2	2	1	0	-1	2	-3	$-1-(2)(2)$ $-1-2=-3$
X	1	0	X	(2)	-3	X	~~$2-(-3)(1)$~~ ~~$2+3=5$~~
0	1	0	0	-3	5	-3	~~$-3=(5)(0)$~~ -3

② 11 mod 13 = 6

Q	A	B	R	T_1	T_2	T	
1	13	11	2	0	1	-1	$0-(1)(1)=$
5	11	2	1	1	-1	6	$1-(-1)(5)$ $1+5=6$
2	2	1	0	-1	6	-13	$-1-(6)(2)$ $-1-12=-13$
X	1	0	X	(6)	-13	X	

③ $10 \bmod 11 = -1$ $\quad -1 \bmod 11 = 12$

Q	A	B	R	T_1	T_2	T	
1	11	10	1	0	1	-1	$0-(1)(1)$ $=-1$
10	10	1	0	1	-1	11	$1-(1)(0)$ $1+10$ $=11$
X	1	0	X	-1	11	X	

④ $11 \bmod 26 = -7 = 19$

Q	A	B	R	T_1	T_2	T	
2	26	11	4	0	1	-2	$0-(1)(2)$ $=-2$
2	11	4	3	1	-2	5	$1-(-2)(2)$ $1+4=5$
1	4	3	1	-2	5	-7	$-2-(5)(1)$ -7
3	3	1	0	5	-7	26	$5-(-7)(3)$ $5+21=26$
X	1	0	X	-7	26	X	

$-7 \bmod 26 = 19$

$(19-26) \bmod 26$

$19 \bmod 26 - 26 \bmod 26$

$= 19 - 0$

Trick:

$26-7 = 19$

18/8/2022

CRT - RSA

DOMS | Page No. | Date / /

Dec(c, d, P, q, x)

$c^d \bmod P = Q_p \Rightarrow \boxed{c^d \equiv Q_p \bmod P}$ → ①

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

$c^{x(p-1) + d \bmod (p-1)} \bmod P$

$= c^{x(p-1)} \bmod p \cdot c^{d \bmod (p-1)} \bmod P$

$Q_p = c^{d \bmod (p-1)} \bmod P$ ~~111~~ $Q_q = c^{d \bmod (q-1)} \bmod q$

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

$\boxed{c^d = Q_q \bmod q}$ → ②

Apply CRT

$n_1 = P \quad N_1 = q$

$n_2 = q \quad N_2 = P$

$N = P \cdot q$

$c^d = \left[\left(c^{d \bmod P-1} \bmod P \right)_{N_1} \right]_{N_1^{-1}}$

$q\,(q^{-1} \bmod P) +$

$(c^{d \bmod q-1} \bmod q)_{a_2} (P^{-1} \bmod q)_{N_2^{-1}}$

a_1

4 times faster than $c^d \bmod n$

CRT - RSA

one way function (easy, efficient → Polynomial time)

$f: X \to Y$

Hash function is one-way fn.	Forward → easy, effi
$H(x) = y \Rightarrow O(256)$	Backward → difficult hard
$O(2^{256}) \Rightarrow$ Exponential hard time	It take exponential time

$2^{40} = \frac{1}{60 \times 60 \times 365 \times 35}$

Trapdoor one-way function:

$f: X \to Y$

Forward → Easy

Backward → Also easy if secret Trapdoor is given

RSA - hard Problem

$f(m) = c = m^e \bmod n$

Given c, e, n, find m is hard (Takes exponential time)

Given m, compute f(m) is easy (Takes polynomial time)

with

Broad casting:-

$m^3 = c_1 \bmod n_1 \rightarrow (1)$

$m^3 = c_2 \bmod n_2 \rightarrow (2)$

$m^3 = c_3 \bmod n_3 \rightarrow (3)$

using CRT we can compute

$m^3 \; n_1 n_2 n_3$

(1) $\Rightarrow m < n_1$

(2) $\Rightarrow m < n_2$

(3) $\Rightarrow m < n_3$

$\therefore m^3 < n_1 n_2 n_3$

$1 < e < \phi(n)$

choose 1. $\phi(n) \Rightarrow$ (Odd no)

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

$e = 3$ (Public key)

$c_1 = m^3 \bmod n_1 \Leftarrow p_1 q_1 = n_1$ (Prime no.)

$c_2 = m^3 \bmod n_2 \quad p_2 q_1 = n_2$

$c_3 = m^3 \bmod n_3 \quad p_3 q_3 = n_3$

Adversary knows $c_1 c_2 c_3$

$m^3 \equiv c_1 \bmod n_1$

$m^3 \equiv c_2 \bmod n_2$

$m^3 \equiv c_3 \bmod n_3$

choose $\frac{1}{2^{512}}$ or $\frac{1}{2^{100}}$

$neg(n) < \frac{1}{2^{100}}$

$\therefore y = m^3$

$m \rightarrow$ cube root of $y \rightarrow$ It is easy

$GCD(n_i, n_j) = 1, \quad 1 \le i, j \le 3$

Given,

$y = m^i \bmod n, \quad i \ge 3$

y, i, n had to compute m

Quadratic Residue

$x^2 \equiv a \bmod p$

quadratic equation is solvable a is quadratic residue modulo P

$a \equiv x^2 \bmod P \Rightarrow QR \; (1)$

If not solvable then a is quadratic non residue modulo P

a is QNR (-1)

Eg:-

1 is QR mod 11 $\Leftrightarrow x^2 \equiv 1 \bmod 11$

$x = 1, 10$

2 is QNR mod 11 $\Leftrightarrow x^2 \equiv 2 \bmod 11$

$x^3 \equiv 3 \bmod 11$

3 is QR mod 11 $x^5 = 5, 6$

$x \rightarrow$ solution

$(P-x) \rightarrow$ Also solution

1
2
3
4
5
6
7
8
9
10

5 possibilities.

$\frac{11-1}{2} = \frac{10}{2} = 5$

$\sqrt{64} = \pm 8$

$+8 \longleftrightarrow -8$

$a = \sqrt{x}$

$a \bmod p = \sqrt{x} \bmod p$

$\left(\frac{p-1}{2}\right)$ a (p-a)

R $\sqrt{x} \bmod p$

$p = 11$

$a = 1$ $p-a = 11-1 = 10$

$16 \rightarrow 5$ | $a = 5$ $p-a = 11-5 = 6$

$49 \rightarrow 5$ | 25 36

3 3

$\sqrt{3} = 5, 6$

Euler's criteria:

a is QR mod P

if $a^{\frac{P-1}{2}} \bmod P = 1$ $a^{\frac{P-1}{2}} \equiv 1 \bmod P$

then a is QR mod P

a is QNR mod P

$1^2 = 1$ 1

$2^2 = 4$ 4

$3^2 = 9$ 4

$4^2 = 16$ 3

13

P

$x^2 \equiv a \bmod p$

$x = a^{\frac{p+1}{4}} \bmod p \qquad p \equiv 3 \bmod 4$

$\left(a^{\frac{p+1}{4}}\right)^2 \equiv a^{\frac{p+1}{2}} \equiv a \bmod p$

$a^{\frac{p+1}{2}-1} \equiv 1 \bmod p$

$a^{\frac{p-1}{2}} \equiv 1 \bmod p$

9/8/2022

Security Means

→ Given cypertxt C, hard to find private key adversary can find in some other way

→ Given cypertxt C, " " corresponding plaintext. adversary can/may be find some part of plaintext.

→ Given cyphertxt C, adversary will not be knowing anything abt plaintext

Shannon

① Perfect security: ciphertxt does not reveal anything about plaintxt

$$P(M=m) = P\left(M=m \,/\, C=c\right)$$

⇓

It mean this C does not give any info/-

② Encryption scheme is perfectly secure if and only if

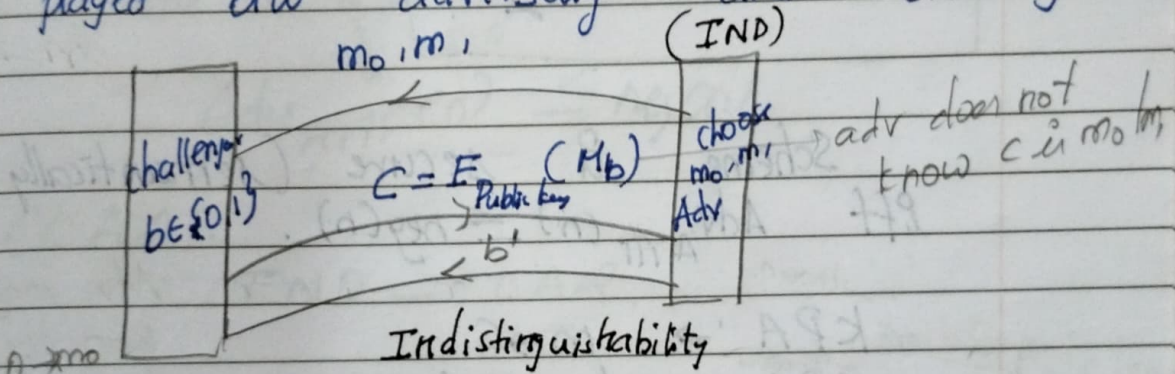
$P(C=c/M=m) = P(C=c/$

$P(M=m_0/C=c) = P(M=m_1/C=c_i) =$ constant

M → Message space.
C → Ciphertext

① = ②

③ It is equivalent to following game played b/w adversary and challenger.



$Adv_{A,\pi}(n)$ (Advantage of adversary)

$= P[b = b'] - \frac{1}{2}$

Scheme is perfectly secure if and only if

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

DOMS | Page No.
Date / /

One time key (OTk)

$C = M \oplus k$ (in this case every M need unique key but it is not practical)

Result:-

Perfectly secure scheme is not practical.

$$Adv_{A,\Pi}(n) \leq \frac{1}{2^{80}} < neg(n) \Rightarrow$$ Game get proved like this

Scheme is secure (semantically secure) iff $Adv_{A,\Pi}(n) \leq neg(n)$.

known
KPA : $m \Rightarrow C$
chosen
CPA : choice $m \rightarrow C$

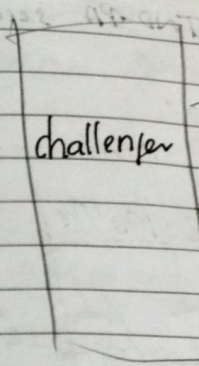
known chosen
KCA : $C \rightarrow M$
CCA : choice $C \rightarrow M$
CCA2 : " $C \rightarrow m$ (Adaptively)
used in Public key cryptography

Adv may be knowing ciphertext & correspond P

IND & IND-CPA

known ~~CPA~~
Public key cryptosystem adv cleat Plaintext & correspond C
CPA & KPA is not useful in public key cryptography
" " useful in symmetric key.
KCA → also not used in public.

CCA



sche

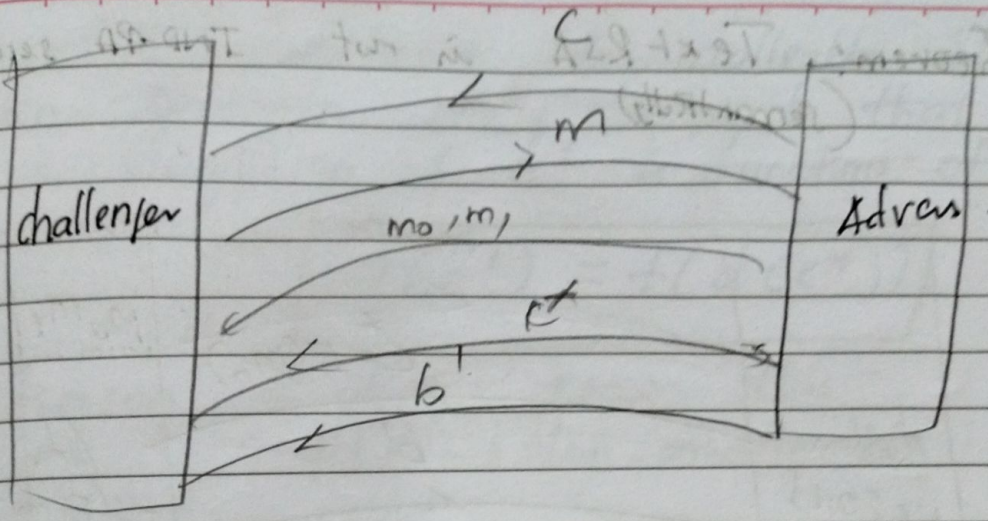
CCA

challeng

Def

Sa

CCA



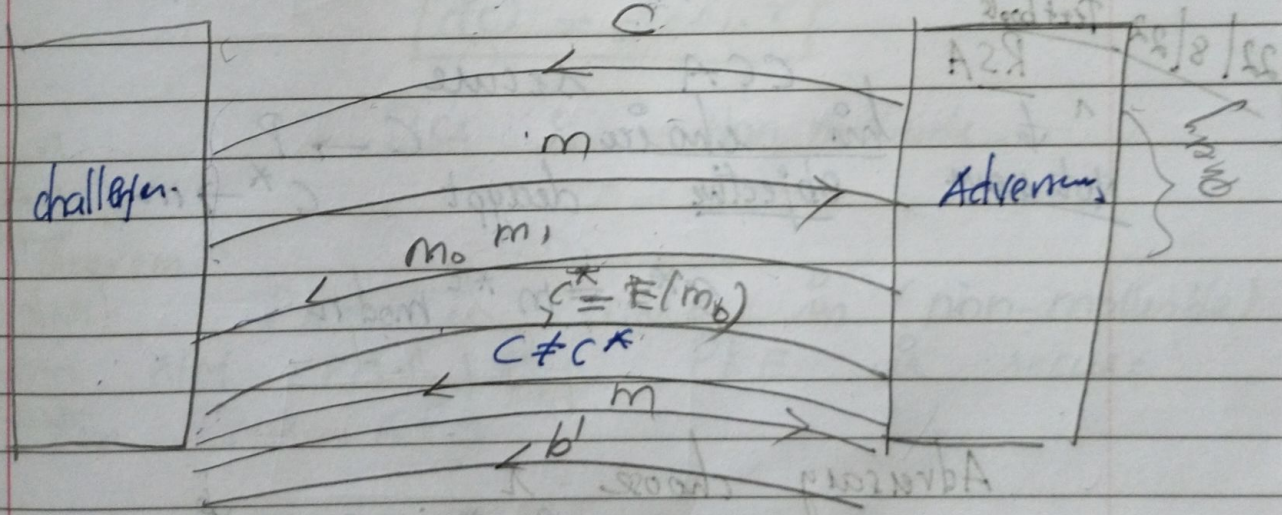
IND – CCA

scheme is IND – CCA secure iff

$Adv_{A,\Pi}(n) \leq neg(n)$

CCA2:

IND – CCA2:



Def:-

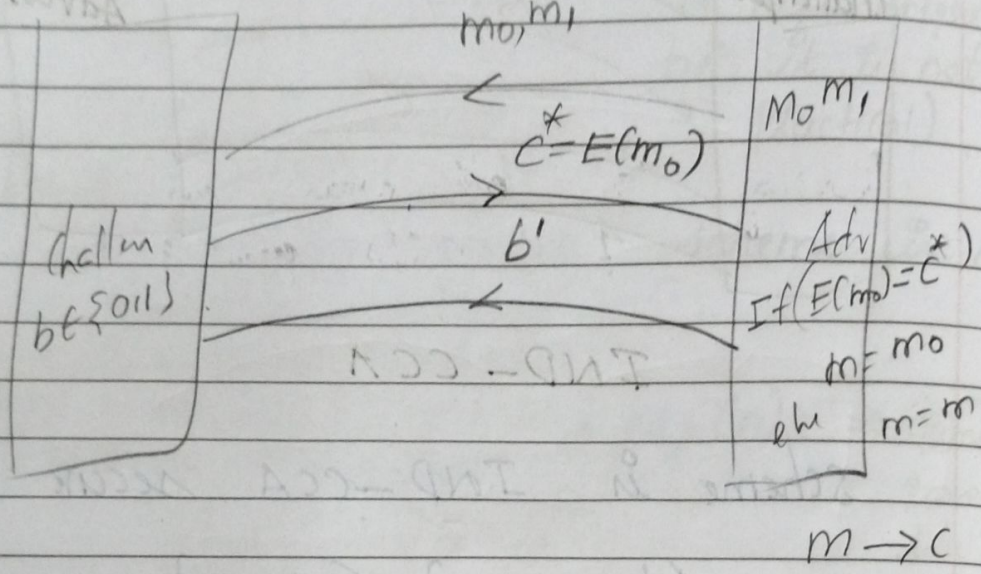
scheme is IND – CCA2 secure iff

$Adv_{A,\Pi}(n) \leq neg(n)$

Same Msg alway same ciphertext ⇒ deterministic

RSA → deterministic

Theorem: Textbook RSA is not IND-CPA secure (semantically)



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

All public key s/m → Randomized.

22/8/22 Textbook RSA

↑ ↓ Not secure

CCA secure

bit choice objective

$C \to P$

$c^* \to m$ (he want to know m)

decrypt

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

(ask chose friend to decrypt)

↑ had to find.

Adversary choose r

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

ask plaintext for c

answer is $m = rm^e$

he knows r, m

compute $m^* = r^{-1}m$

Malleability:

PKE scheme is malleable if adversary can transform $c^* \to c'$ such that decryption of c' is function of $d(c^*)$

$$\boxed{d(c') = f(d(c^*))}$$

adversary should not know this

∴ PKE → Non-malleable

Show that RSA is malleable.

$c^* \to c$

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

choose random r

compute $c = r^e c^*$

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

$d(c) = m^* r$ ∵ $d(c^*) = m^*$

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

∴ RSA is Non-malleable.

Theorem:

PKE is secure in (non-malleable) NM-CPA then PKE is secure in IND-CPA

$A \to B \iff \neg B \to \neg A$

↳ Prove this (This should be easy)

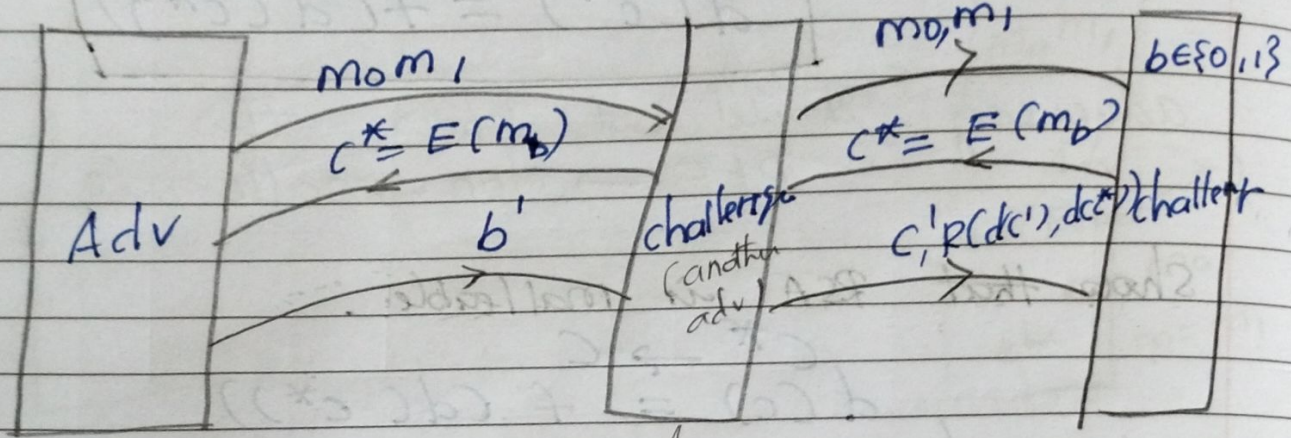
NM-CPA → IND-CPA

Adversary can break PKE in IND-CPA

⇒ " can break PKE in NM-CPA (with Non-negligible prob in polytime)

Prove this

(Breaking in exponential time is not taken as breaking one by one it takes)
(so do break in polynomial time)



→ does not know b
→ forward same c^* to Adv.
→ ~~$E_b(m_b' + 1) = c'$~~

$$E(m') = c'$$

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

$$\boxed{m' = m_b^* + 1}$$

Theorem:- A (This also true) Vice Versa

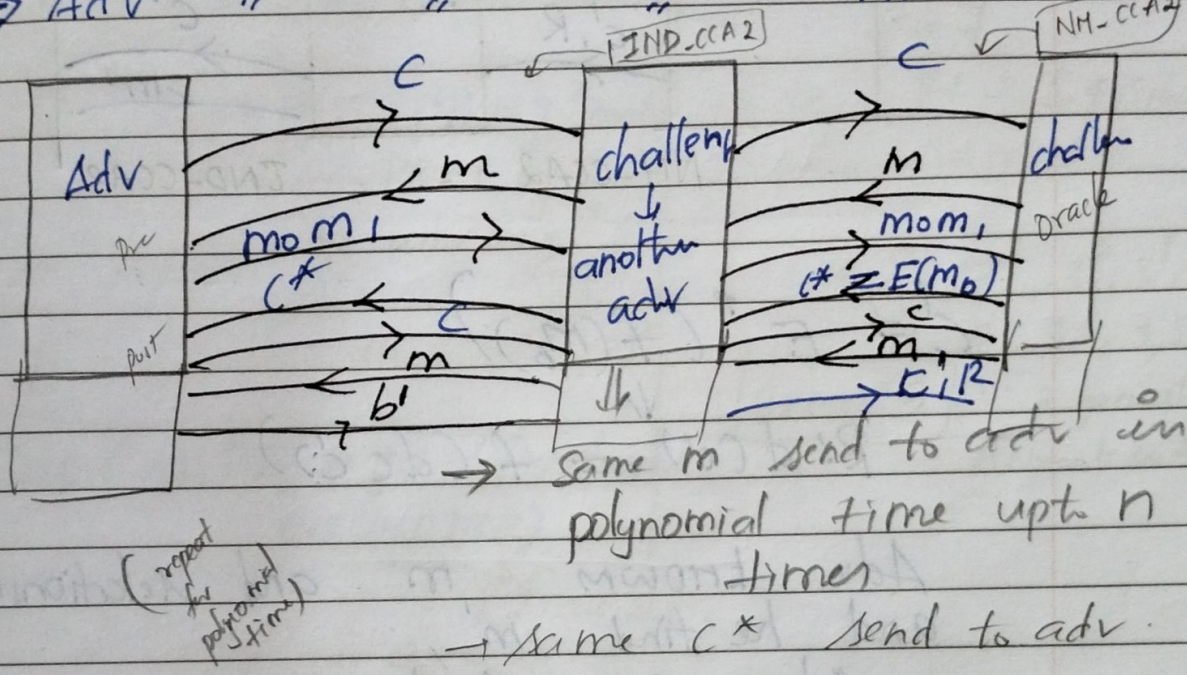
PkE is secure in NM-CCA2 $\Leftrightarrow$ PkE is secure in IND-CCA2

NM-CCA2 $\Rightarrow$ IND-CCA2 B (If this is true)

$A \rightarrow B$

$\neg B \rightarrow \neg A$

Adv can break PkE in IND-CCA2 $\Leftrightarrow$ Adv " " " " NM-CCA2 (if 1 another)



(repeat for polynomial times)

$\Rightarrow$ Same m send to adv in polynomial time upto n times

$\rightarrow$ same c^* send to adv.

$E(m') = c'$

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

$\boxed{m' = m_{b'}^* + 1}$

$c' = E(f(m_b))$

$\downarrow$

$E(m_b + 1)$

$\Rightarrow$ Relationship.

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

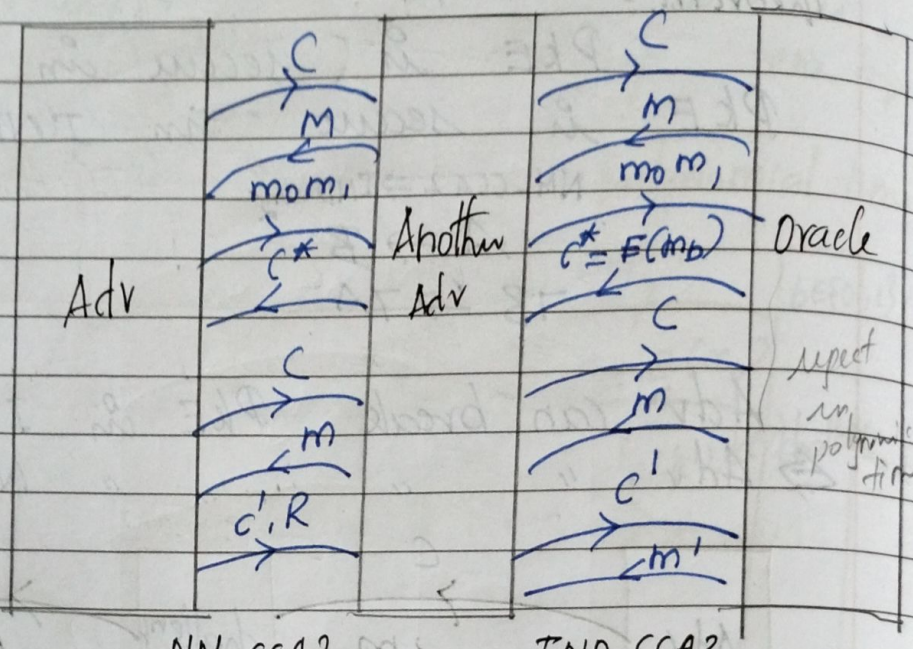
$m' = m_b^* + 1$

26/8/22.

Reverse proof :-

IND-CCA2 $\rightarrow$ NM-CCA2

If adv can break scheme in NM-CCA2 then $\exists$ another adv who can break scheme in IND-CCA2

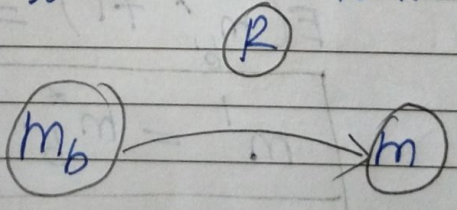


NM-CCA2 IND-CCA2.

$$c' = E'(f(m_b))$$

$$R: d(c') = f(dc\,c')$$

Adv knows m, m' and relationship R and he find m',
Adv can find m_b, m_b will be (m_0, m_1)
b will be either 0 or 1



NM-CPA ← NM-CCA ← NM-CCA2 (strongest, adaptive)
↓↑ No proof ↓↑ No proof ↕ This is
IND-CPA ← IND-CCA ← IND-CCA2 Pro
⇓ publickey cryptogra

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

ElGamel: P = 1024 bit (size)

Public Parameter:
Cyclic group Z_p with generator g.

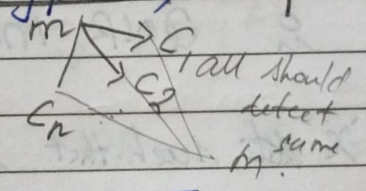
$Z_p = \{1, 2 \ldots P-1\}$ *mod P
abo form cyclic group

$P = 7$
$Z_7 = \{1,2,3,4,5,6\}$ *mod 7
$= \{3, 3^2, 3^3, 3^4, 3^5, 3^6\}$
$3, 2, 6, 4, 5, 1$
Generator 3 (∵ 3 gen all elements in Z_7)

KeyGen (1^n): choose $x \in \{2, P-2\} \neq 1, P-1$

$PR = x$ $PB = g^x \bmod p$
$PB = 1$ by fermat thm
to adv can choose $p-1$
so avoid $(1, P-1)$

Enc $(m, PB_R = y)$: (Randomized encryption)



$M \in Z_p$, $C \in Z_p$

Choose $k \in \{2, P-2\}$ Randomly.
$C_1 = g^k$, $C_2 = m \cdot y^k$

Dec (C_1, C_2, x):
compute $\frac{C_2}{C_1^x}$

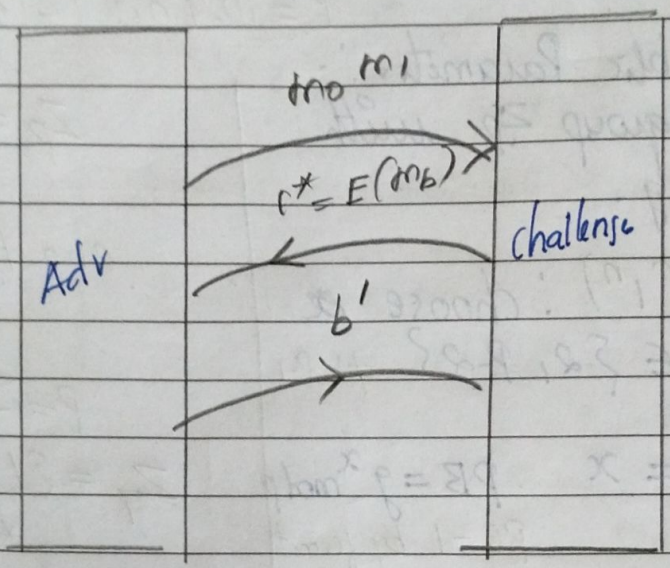
$= C_2 (C_1^x)^{-1}$
find this in Z_p

$y^k = g^{xk} = (g^x)^k$
random
$= (g^k)^x$
$\downarrow C_1$
here with see

oracle
upect in polynomial time.
ship R
will be
0 or 1
orgeot, adaptive
- CCA 2
↕ This is
- CCA 2 Provi
key cryptogra
once he can answer based on answer he can ask another query
dep on answer

Ex

Elgamal is not IND-CPA secure.



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

Adv: Advantage, A: Adversary, Π: protocol

= Non-malleable

Ex:

g is QNR mod p

Not exit ~~Exx~~ x' ~~dd~~ such that $x^2 \equiv g \bmod p$

iff (or)

$g^{\frac{p-1}{2}} \equiv -1 \bmod p$ $\quad \left(\frac{g}{p}\right) = -1$

(or)

$g^{\frac{p-1}{2}} \bmod p = -1$

g is generator of cyclic group Z_p

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

$p-1 \rightarrow$ smallest one

ord = least no. d s.t $(g^{p-1} = 1)$

$$O(g) = p-1$$

Proof by contradiction

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

$$g^{\frac{p-1}{2}} \bmod p = 1 \text{ or } -1$$

if $g^{\frac{p-1}{2}} \bmod p = 1 \Rightarrow ord(g) = \frac{p-1}{2}$.

$\Downarrow$

contradict the assumption

so $g^{\frac{p-1}{2}} \bmod p = -1$

Eg:-

g is QNR mod p $\Rightarrow \left(\frac{g}{p}\right) = -1$

$C_1 = g^k$, $C_2 = m y^k$

Case 1:

y is QR mod p $\Rightarrow \left(\frac{y}{p}\right) = 1$

$y^k = +1$

$C_2 \leftrightarrow m$ | if C_2 is QNR then m also QNR.

Adv choose of msg

$m_b = QR(p)$

$m_{1-b} = QNR(p)$

Case 2:

y is QNR mod p $= \left(\frac{y}{p}\right) = -1$

$C_1 = g^k$ check whether C_1 is QR or QNR mod P

Case a:

If C_1 is QR $\Rightarrow$ k is even

then $g = -1$ so $(-1)^k = 1$

y^k is 1

$C_2 \leftrightarrow m$ (C_2 same as m)

Case b:

If C_1 is QNR $\Rightarrow$ k is odd.

then $g = -1$ so $(-1)^k = -1$

If C_2 is QR then m is QNR.

If C_2 is QNR then m is QR.

Modified Elgamal:-

Schnoorr ~~Shorr~~ cyclic group:

$\frac{P-1}{2} = \frac{7-1}{2} = \frac{6}{2} = 3$ (also prime)

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

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

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

$\boxed{g = 3}$ $\{2 \quad 4 \quad 1\}$

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

cyclic subgroup of $Z_7 = G$

(Schnorr Group)

Elgamal is malleable.

Schnorr group choose prime P, q such that (q divides P-1). [P-1 = 2·q].
Cyclic subgroup of order q is called Schnorr group.

PP: Cyclic Z_p with generator h.

$$Z_p = \{h_x \cdots h^{P-1} = 1\}$$

$$g = h^2$$

Cyclic group G with generator g.

$M \in G$ $\quad$ $C \in G$

$M = \{2, 4, 1\}$ $\quad$ $C = \{2, 4, 1\}$

g is QR mod P

also m is QR mod P

" c is QR mod P

Modified Elgamal:

PP: cyclic group G with gen g

KeyGen(1^n): choose $x \in \{G-1\}$ $PR = x$

$PB = g^x$

Enc(m, $PB_R = y$): Randomized encryption

choose: $k \in \{2, P-2\}$ randomly.

$c_1 = g^k$ $\quad$ $c_2 = m y^k$

Dec(c_1, c_2, x): Compute $\frac{c_2}{c_1^x} = c_2 (c_1^x)^{-1}$

Proof Elgamal is not CCA secure

$C_1^* = g^k \quad C_2^* = my^k \Rightarrow (m)$

$C' = (C_1', C_2') \rightarrow m'$ (oracle gives m' by decrypting)

$C_1' = g^k \quad C_2' = 2 \cdot C_2^* \Rightarrow (mr)$ (oracle gives mr)

Proof Elgamal is malleable: