21/08/22

Books :

1. Modern Cryptography
   → Jonathan Katy & Lindell

2. Modern Cryptography
   ~~&~~ Theory & Practice
   → Wen Bo Mao

Course Evaluation Scheme :

CT1 - 20
CT2 - 20
Demo - 20 (maybe 2 projects).
Semester - 40

Objective of Cryptography :

secure communication btw 2 parties even in the presence of an adversary

Private key cryptosystem

Before 1976 (used still) → Symmetric Cryptography

(Eg) :- AES, DES, RC4

Pre-requisite :- Common key problem : parties must meet in person to share the key securely

Important properties of symmetric

(1) Confidentiality of message ; → Block / Stream

(2) Authentication.

2 types of cryptosystems :

- ✓ Block cipher (Eg: AES).
- ✓ Stream cipher

Authentication → MAC (Symmetric / private).

Symmetric system (AES, RC4) → much more simpler, efficient than asymmetric systems (RSA, El-Gamal).
⇒ So 95% of the times, symmetric systems are used (but for the situation is opposite when it it comes to research).

Public Key Cryptosystem

→ Soln for sharing key in person (in the case of symmetric systems)

→ Proposed first by Diffie Hellman in 1976.

Every user - has a private and public key
Encryption - done using both keys
Decryption - done using both keys but decryption keys have to be different from encryption key

$S \longrightarrow R$
(S encrypts msg using R's public key ⇒ only those who have R's private key can decrypt the ciphertext)

$Enc(m, PB_R) \rightarrow C$

$Dec(C, PR_R) \rightarrow m$.

Basics

① Private key cryptosystems :
- RSA
- El-Gamal
- ECC (lightweight ← Elliptic curve) used in Blockchain)

② Authentication → Digital signature
- RSA
- Schnorr signature

Advanced

③ Blockchain 1.0 (cryptocurrency - Bitcoin)

Blockchain 2.0 (Ethereum, Smart contract) → Attacks (Dos attack)

④ Zero Knowledge Proof

(Convincing the verifier that you have a secret msg without revealing it).

↓

has many applications in Blockchain

Optional

⑤ Multiparty computation (MPC).

→ 2PC - given by Yao

discrete
Date
Page

He proposed a fn $f(x,y)$ that takes 2 secret msgs x,y and returns an answer without revealing anything about x,y

1978 → RSA Algorithm
(Rivest, Shamire, Adleman).

KeyGen(1^n):
n - key size (security parameter)
if $n=20$, it can be easily broken by Brute force

For RSA, $n=1024$. (So 2^{1024} possibilities).

Choose 2 primes p,q (each of around 512 bits)
Compute $n=pq$ (around 1024 bits).

$\phi(n)$ is the #integers $< n$ and relatively prime to $n \Rightarrow \gcd(a,n)=1$

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

Let $n = p_1^{x_1} p_2^{x_2} \cdots p_i^{x_i}$ where $p_1, p_2, \ldots, p_i$ are primes

Theorem: (Any n can be expressed as a product of its prime factors)

Then $\phi(n) = (p_1^{x_1} - p_1^{x_1-1})(p_2^{x_2} - p_2^{x_2-1}) \cdots (p_i^{x_i} - p_i^{x_i-1})$

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

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

$= (4-2)(5-1)$

$= 8.$

12/08/22

RSA Algorithm

Key Gen (1^n):

Choose 2 primes p, q

Compute $n = pq$

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

choose e such that $GCD(e, \phi(n)) = 1$.

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

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

Public Key = (n, e)

Private Key = (p, q, d).

$n = pq$

multiples of p = $p, 2p, 3p, \ldots, qp$

multiples of q = $q, 2q, 3q, \ldots, pq$

No. of numbers that are not relatively prime to n = $p + q - 1$

pq is common

$\therefore$ # nos such that gcd with n is 1 =

$pq - (p + q - 1)$

$pq - p - q + 1$

$= (p-1)(q-1)$

Enc(m, n, e) :

$C = m^e \bmod n$

Dec(c, p, q, d) :

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

Correctness of RSA :

Correctness criteria

Show that $Dec(Enc(m)) = m$

$$Dec(c, p, q, d) = c^d \bmod n$$
$$= m^{ed} \bmod n$$

~~Case i~~:

Message space = $\{0, n-1\}$
Ciphertext space = $\{0, n-1\}$

First encode the message as a number $m \in \{0, n-1\}$. We then encrypt this encoded m.

Case 1 : $GCD(m, n) = 1$

$\Rightarrow$ m is not a multiple of p or q

Euler's theorem :

$m^{\phi(n)} \equiv 1 \bmod n$ if $GCD(m, n) = 1$.

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

↓

(divides)

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

Fermat's theorem :

If n is prime then

$m^{n-1} \bmod n = 1$.

For correctness

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

$\Rightarrow m^{ed-1} \bmod n = 1$.

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

$\rightarrow ed \equiv 1 \bmod \phi(n)$

$\Rightarrow \phi(n) \mid ed - 1$.

so $ed - 1 = k\phi(n)$.

$m^{ed-1} \bmod n = 1$

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

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

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

$\Rightarrow m = p, 2p, \ldots, p(q-1), q, 2q, 3q, \ldots, (p-1)q$ (m cannot be n, $m \in \{0, n-1\}$)

(a) Let $m = ip$

By Fermat's theorem

$m^{q-1} \bmod q = 1$ (bcos $GCD(p,q) = 1$ $\Rightarrow GCD(m,q) = 1$. (as $GCD(i,q) = 1$).

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

$$\Rightarrow m^{(q-1)(p-1)} \bmod q = 1.$$

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

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

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

$m \cdot m^{\phi(n)} = m + \underbrace{ipqt}_{=m}$ (Multiplying m on both sides).

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

$m^{ed} = m + itn$

Take modulo n on both sides

$m^{ed} \bmod n = m$ ($itn \bmod y = 0$)

($m < n$

So $m \bmod n = m$)

Chinese Remainder Theorem :

Let $x \equiv a_1 \bmod n_1$

$x \equiv a_2 \bmod n_2$

$\vdots$

$x \equiv a_k \bmod n_k$

such that $GCD(n_i, n_j) = 1 \quad 1 \leq i, j \leq k$

We have to find x

Method :

Find $N = n_1 n_2 \ldots n_k$ and

$$N_1 = \frac{N}{n_1}, \quad N_2 = \frac{N}{n_2}, \ldots, N_i = \frac{N}{n_i}$$

$\Rightarrow GCD(N_i, n_i) = 1.$

$\Rightarrow$ ~~there~~ $N_i^{-1} \bmod n_i$ exists

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

$N_1 (N_1^{-1} \bmod n_1) \bmod N \neq 1.$

both should be same for it to be 1.

(Ex): $2^{-1} \bmod 3 = 2.$

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

$\equiv 4. \neq 1.$

1. $x \bmod 3 = 2$

$x \bmod 5 = 3$

$x \bmod 7 = 2$

$N = 3.5.7 = 105$

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

$x = [2.35(35^{-1} \bmod 3) + 3.21(21^{-1} \bmod 5) + 2.15(15^{-1} \bmod 7)] \bmod 105.$

Note: $x_1 \circledast x_2 \bmod n = (x_1 \bmod n \circledast x_2 \bmod n) \bmod n$

(Applicable for +, −, ×, and inverse also)

$$x : [3[70((35 \bmod 3)^{-1} \bmod 3) + 63((21 \bmod 5)^{-1} \bmod 5) + 30((15 \bmod 7)^{-1} \bmod 7)]] \bmod 105$$

$$= (70(2^{-1} \bmod 3) + 63(1^{-1} \bmod 5) + 30(1^{-1} \bmod 7)) \bmod 105$$

$$= (140 + 63 + 30) \bmod 105$$

$$= 233 \bmod 105$$

$$= 23.$$

18/08/22 CRT-RSA :

In RSA, we do not use the private keys p, q for decryption

In CRT-RSA, p, q are used in the decryption algo to improve security

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

Compute $C^d \bmod p = Q_p$

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

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

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

By Fermat's theorem

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

$\therefore \boxed{C^{d \bmod (p-1)} \bmod p = Q_p} \quad \cdots (1)$

CRT-RSA has same time complexity as RSA but has a smaller constant factor (Bcos we find $C^{d \bmod (p-1)}$ and not C^d and $d \geq d \bmod (p-1)$).

Illy $\boxed{Q_q = C^{d \bmod (q-1)} \bmod q} \quad \cdots (1')$

$C^d \equiv Q_p \bmod p \longrightarrow (1)$

$C^d \equiv Q_q \bmod q \longrightarrow (2)$

Use CRT

$N = pq$

$n_1 = p, \quad n_2 = q, \quad N_1 = q, \quad N_2 = p$

$$C^d \equiv \Big[\big(C^{d \bmod (p-1)} \bmod p \big) \, q \, (q^{-1} \bmod p) + \big(C^{d \bmod (q-1)} \bmod q \big) \, p \, (p^{-1} \bmod q) \Big] \bmod pq$$

$a_1 = Q_p \quad N_1 \quad N_1^{-1} \bmod n_1$

$a_2 = Q_2 \quad N_2 \quad N_2^{-1} \bmod n_2$

N

CRT-RSA is 4 times faster than RSA as it deals only with smaller numbers (powers, ...)

Hard problems

1. One way function :

$$f : X \to Y$$

Given X, $f(X)$ can be computed in polynomial time (efficient).

Given Y, finding X such that $Y = f(X)$ is hard (⇒ takes exponential time)

possible but takes many years.

(Eg): Hash functions

2. Trapdoor one-way function :

$$f : X \to Y$$

Given X, $f(X)$ can be found easily

Given Y, finding X such that $Y = f(X)$ is easy

if trapdoor is given
↓
some secret

RSA is based on trapdoor functions

RSA - hard problem

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

Given C (found by intercepting the channel say).

Given C, e, n (e, n → public keys).
it is hard to find m

Trapdoor here is (P, Q) or d which can be used to compute m.

Specific cases when RSA can be broken

1. ~~Broad Dest~~ Broadcasting:

$1 < e < \phi(n)$

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

Negligible fn : $\frac{1}{\text{exponential fn}}$

$\text{neg}(n) < \frac{1}{2^{100}}$ (changes over time as speed of systems increase)

If 3 people choose 3 sets of prime factors

$p_1 q_1 = n_1$

$p_2 q_2 = n_2$

$p_3 q_3 = n_3$.

Also, they choose the same public key $e = 3$ say

Probability of 2 people choosing ~~the~~ 1 same prime factor $= \frac{1}{2^{512}}$ (say keys are 512 bits)

$< \frac{1}{2^{100}}$ ($\Rightarrow$ negligible).

So it is safe to assume all prime numbers are distinct.

If we send a message m to all 3 of them then

$c_1 = m^3 \bmod n_1$

$c_2 = m^3 \bmod n_2$

$c_3 = m^3 \bmod n_3$

→ $m^3 \equiv C_1 \bmod n_1$

$m^3 \equiv C_2 \bmod n_2$

$m^3 \equiv C_3 \bmod n_3$

To use CRT,

$GCD(n_i, n_j) = 1$ $\quad \forall i,j \in \{1,2,3\}$

$1 \le i, j \le 3$

since no 2 primes are equal (only negligible chance), we can apply CRT.

$\therefore m^3 \bmod \underbrace{(n_1 n_2 n_3)}_{=N}$ can be computed using CRT.

We send m to all 3 people

since message space is $\{0, \ldots, N-1\}$

then $m < n_1$, $m < n_2$ and $m < n_3$.

$\Rightarrow m^3 < n_1 n_2 n_3$

So $m^3 \bmod (n_1 n_2 n_3) = m^3$.

$\therefore$ By using CRT we find

$Y = m^3 \bmod (n_1 n_2 n_3)$

$= m^3$

$\Rightarrow m = \sqrt[3]{4}$ which is easy to find

Quadratic Residue

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

This eqn can be solved if
a is Quadratic Residue modulo p.
(QR)

Cannot be solved if
a is Quadratic Non-residue modulo p.
(QNR).

(Eg): 1 is QR modulo 11
$\Rightarrow x^2 \equiv 1 \bmod 11$ has solution(s)
$\Rightarrow x = 1, 10$

2 is QNR mod 11
$\Rightarrow x^2 = 2 \bmod 11$ has no solution

3 is QR mod 11
$\Rightarrow x^2 = 3 \bmod 11$ has solution(s)
$\Rightarrow x = 5, 6$.

Note :

1. All quadratic residue eqns have 0 or 2 solutions
2. If x is a soln for QR mod p then $p-x$ is also a soln.
3. $\left(\frac{p-1}{2}\right)$ values are QR mod p and $\left(\frac{p-1}{2}\right)$ values are QNR mod p

1	
2	1
3	
4	
5	
6	
7	
8	
9	
10	

Euler's Criteria

a is QR mod p if

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

Else a is QNR mod p.

⇒ Only a checking condition does not give the soln

Solution is $x = a^{\frac{p+1}{4}} \bmod p$. if $p \equiv 3 \bmod 4$ (Eg: $p = 3, 7, 11$).

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

$$= a^{\frac{p-1}{2}} \cdot a$$

$$\equiv 1 \cdot a \bmod p$$

$$\equiv a \bmod p.$$

⇒ First check if $a^{(p-1)/2} \equiv 1 \bmod p$ then find $a^{(p+1)/4}$.

19/08/22

Security Means.

① Given ciphertext C, it should be hard to find private key (of the receiver).
⇒ Not strong enough
(Adversary can still find some bits of the plaintext & without the key by some other ways?),

② Given ciphertext C, it should be hard to find the corresponding plaintext
⇒ Adversary can still find some bits of the plaintext and tamper with it
(Eg): In a message containing Bank, account details, money, if adversary can only decrypt the amount, he can still change it.

Perfect security :

Requirement
① ✓ Given by Shannon
✓ Ciphertext does not reveal anything about the plaintext

$$P(M=m) = P(M=m \mid C=c)$$

(2) Encryption scheme is perfectly secure iff

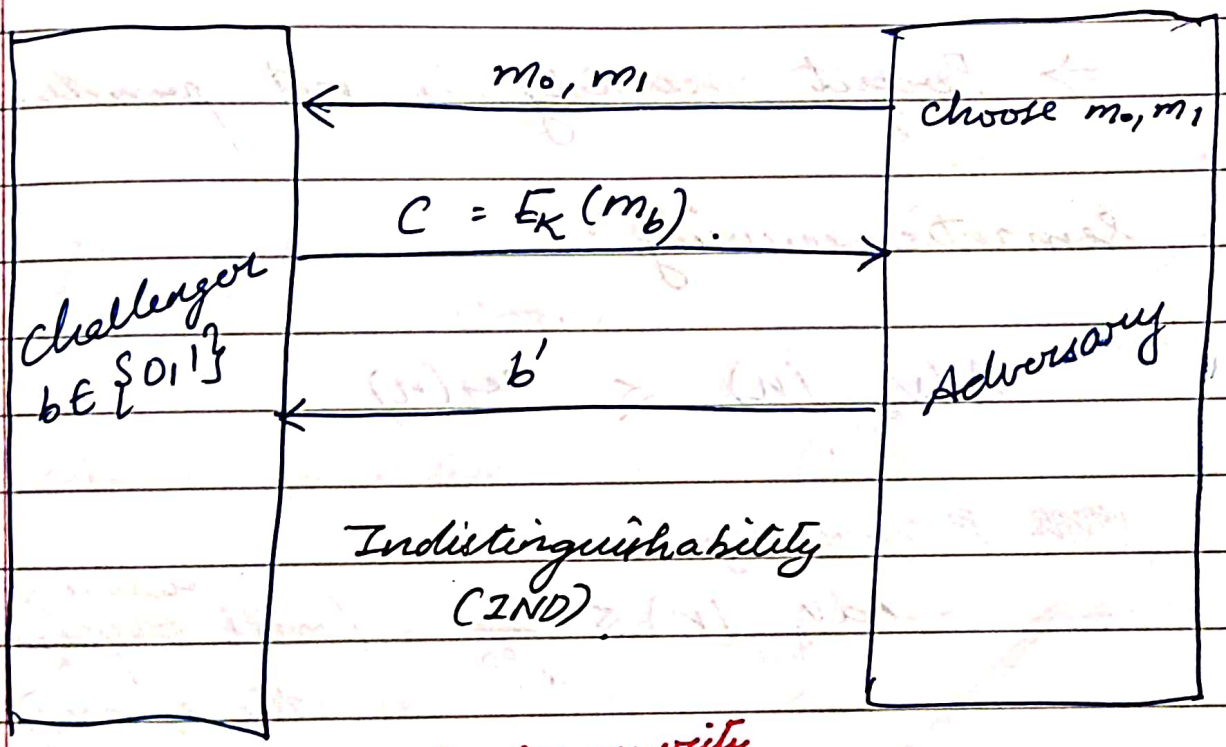
~~$P(C=c \mid M=m_0) = P(C=c \mid M=m_1)$~~.

$P(M=m_0 \mid C=c) = P(M=m_1 \mid C=c) = \text{constant}$

↓ message space

↓ ciphertext space

(3) Equivalent to the following game played b/w Adv. and challenger



$Adv_{A,\Pi}(n) = P(b == b') - 1/2$ (Advantage of adversary under the scheme Π).

↓ encryption scheme

→ factor for security

Scheme is perfectly secure if

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

All 3 defns of perfect security → equivalent

(Eg): OTP

$C = M \oplus K$

(1 Key for ~~every~~ 1 message)

⇒ Perfect security is not practical

Semantic security:

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

Currently

$$Adv_{A,\Pi}(n) \leq \frac{1}{2^{80}}$$ (will reduce further over the years).

∴ New defn:

Scheme is secure (semantically)

iff

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

Classmate
Date
Page

Known plaintext attack (KPA):

Adversary knows plaintext & corresponding ciphertext
(m, c)

Chosen plaintext attack (CPA):

Adversary knows ciphertext of his choice of plaintext
(choice of m, c).

Known ciphertext attack (KCA):

Adversary knows few ciphertexts & their corresponding plaintext
c → m

Chosen ciphertext attack (CCA)

Adv. Knows plaintext corresponding to his choice of ciphertexts
choice of c → m.

CCA2:

~~CCA~~ adaptive CCA
(subsequent ciphertexts are based on knowledge from previous c → m pairs).

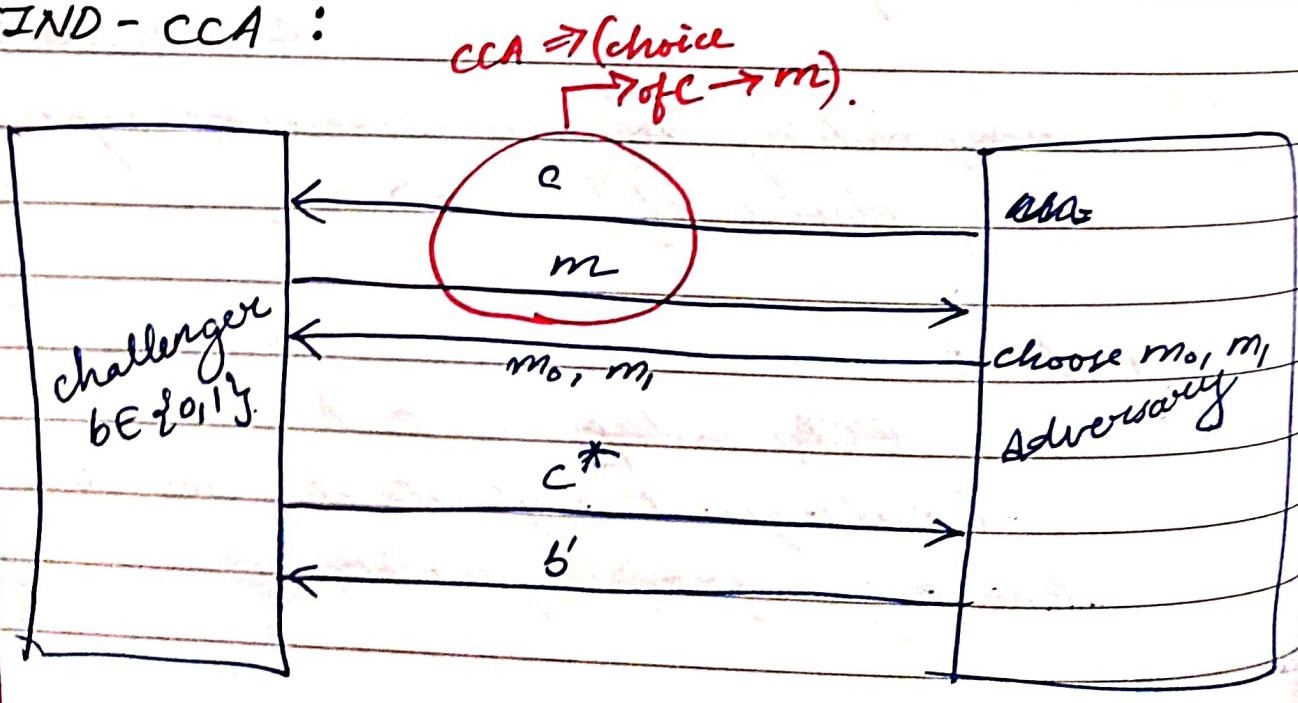
KPA, CPA → no extra info is derived in case of public key cryptosystem.
(In symmetric system key is shared b/w sender & receiver, so KPA, CPA can be used to find that key)

KCA is same as KPA, so no use in public key cryptography

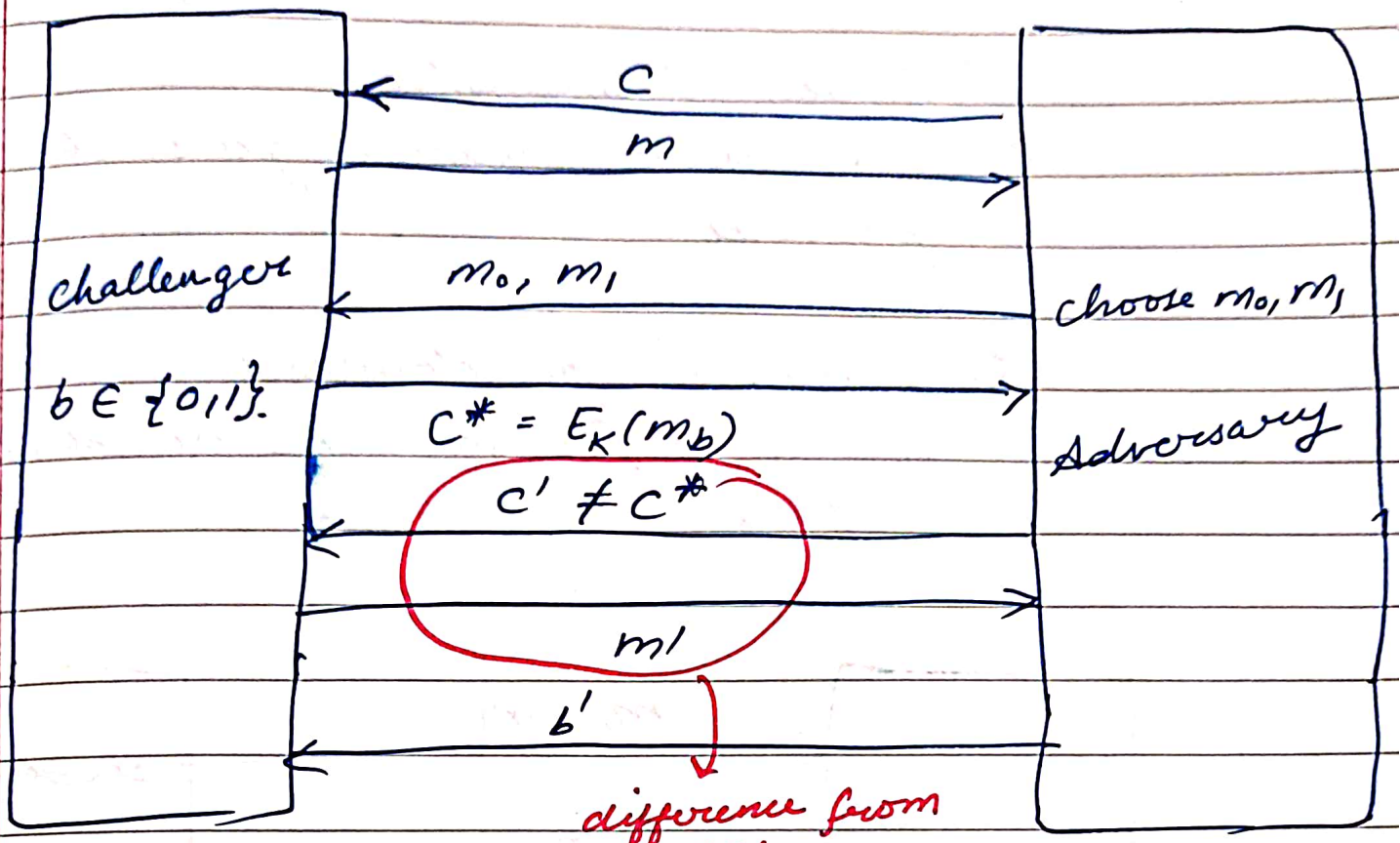
Only CCA, CCA2 are of concern (in public key cryptosystem).

In public key systems :
IND ≈ IND-CPA (coz CPA has no effect).

IND-CCA :



IND - CCA2



Queries ⇒ can only be polynomial (NOT exponential).

Scheme is IND-CCA2 secure if

$Adv_{A,\Pi}(n) \leq neg(n)$ (in the above scheme).

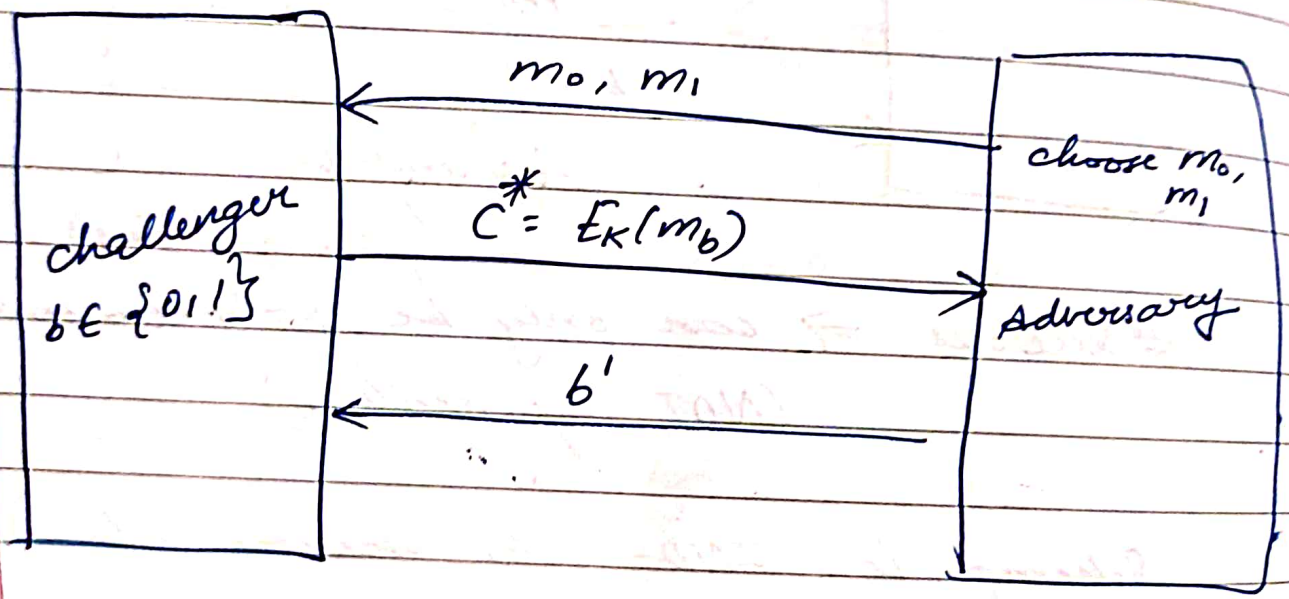
Level of attack (smartness of adversary):

IND-CPA < IND-CCA < IND-CCA2

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

RSA is deterministic
⇒ same message always gives the same ciphertext.

El-Gamal is randomized
⇒ different c for same m at different times.



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

Here both (n, e) are public keys

so adversary can easily find
$c_0 = m_0^e \bmod n$
$c_1 = m_1^e \bmod n$

and simply check if $C^* = C_0$ or $C^* = C_1$

$\Rightarrow$ ~~Bit~~ $P[b == b'] = 1$

$\therefore Adv_{A,\Pi}(n) = 1 - 1/2 = 1/2 > neg(n)$

$\Rightarrow$ RSA is not semantically secure

22/08/22

Any deterministic encryption scheme cannot be IND-CPA (or) semantically secure (same ciphertext for same message always).

RSA is not IND-CCA secure

his choice of $C \longrightarrow P$. (he knows).

Objective : decrypt C^*

$$C^* = (m^*)^e \bmod n$$

Adversary chooses r such that

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

Now adversary asks the plaintext for c which is

$$m = rem^*$$

The adversary knows r and m and can find m^* as

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

So textbook RSA is not IND-CCA2 secure.

Malleability :

Public key Encryption scheme is malleable if adversary can transform C^* to C' such that

$$d(C') = Dec(C') = f(Dec(C^*))$$

malleable ⇒ both the decryptions are related since C' is derived from C^*

otherwise the scheme is non-malleable

(Eg): Adversary should not be able to change the recipient's account to his own

in the ciphertext ⇒ encryption should be non-malleable

Theorem: RSA is malleable

Proof:

Goal: change c^* to c such that $d(c) = f(d(c^*))$.

choose r

Compute $c = r^e c^*$

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

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

$d(c) = m^* r$ } both are related

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

~~textbook~~

So, RSA is ~~not~~ malleable ~~(CPA)~~

~~non-malleable~~

(Practical RSA is non-malleable).

2 security notions

Indistinguishability Non-malleability

Theorem :

A If Public Key Encryption (PKE) scheme is secure in Non-malleable - CPA (or) NM-CPA then PKE is secure in IND-CPA (converse is not known)

B

We have to prove $A \rightarrow B$

$\rightarrow$ ~~we~~ it is enough to prove

$\neg B \rightarrow \neg A$ (contrapositive),

$\rightarrow$ in polynomial time

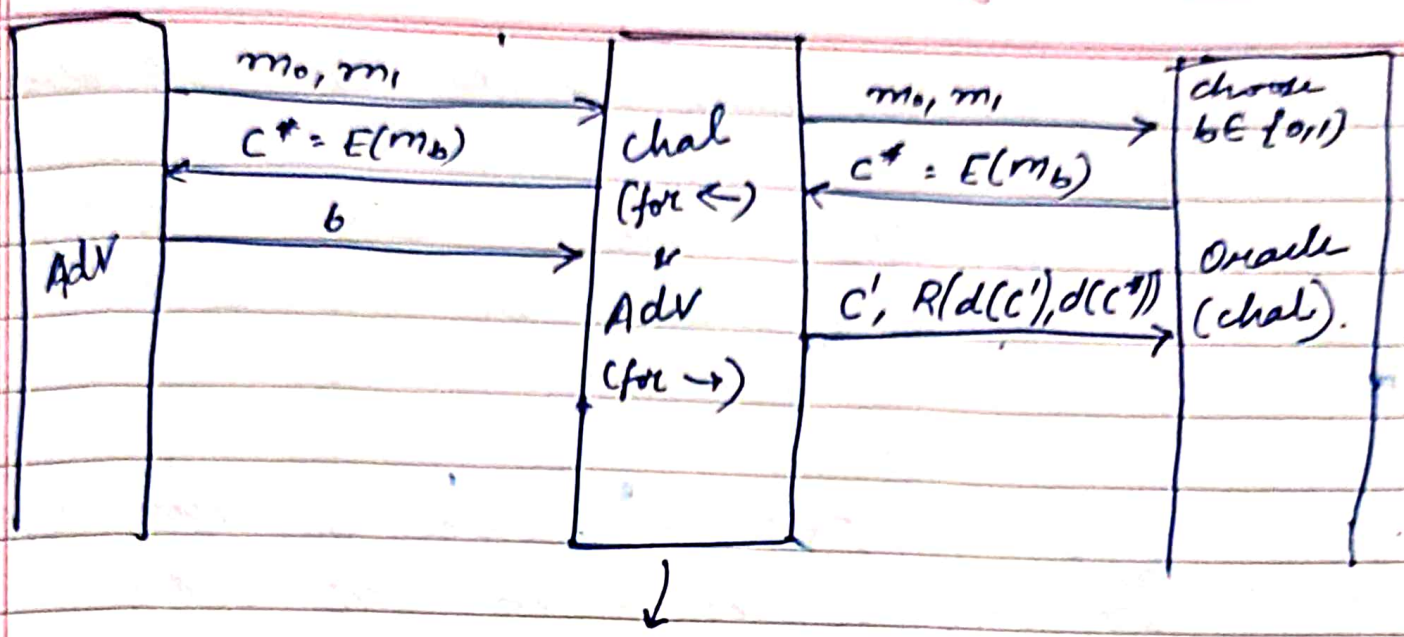
i.e If adversary can break PKE in IND-CPA then adversary can break PKE in NM-CPA

Break $\Rightarrow$ in polynomial (feasible) time with ~~non-negligible~~ non-negligible probability

Adv can break PKE in IND-CPA

$\Rightarrow \Pr(b == b') > 1/2$

$Adv_{A,\Pi}(n) > 0$



He does not know the value of b himself

since scheme is not secure in IND-CPA, we know $b^* = b$.

So challenger gets b from Adv1.

Now Chal has to break PKE in NM-CPA.

since chal knows the message $m_{b'} = m_b$

he can find $c' = E(\underbrace{m_b + 1}_{m'})$.

$= (m_b + 1)^e \bmod n$

$(e, n) \rightarrow$ public keys

m_b is known.

So chall can find c'.

$d(c^*) = m^*$ & $d(c') = m^* + 1$ $\Rightarrow$ both are related

Thus we can break NM-CPA also

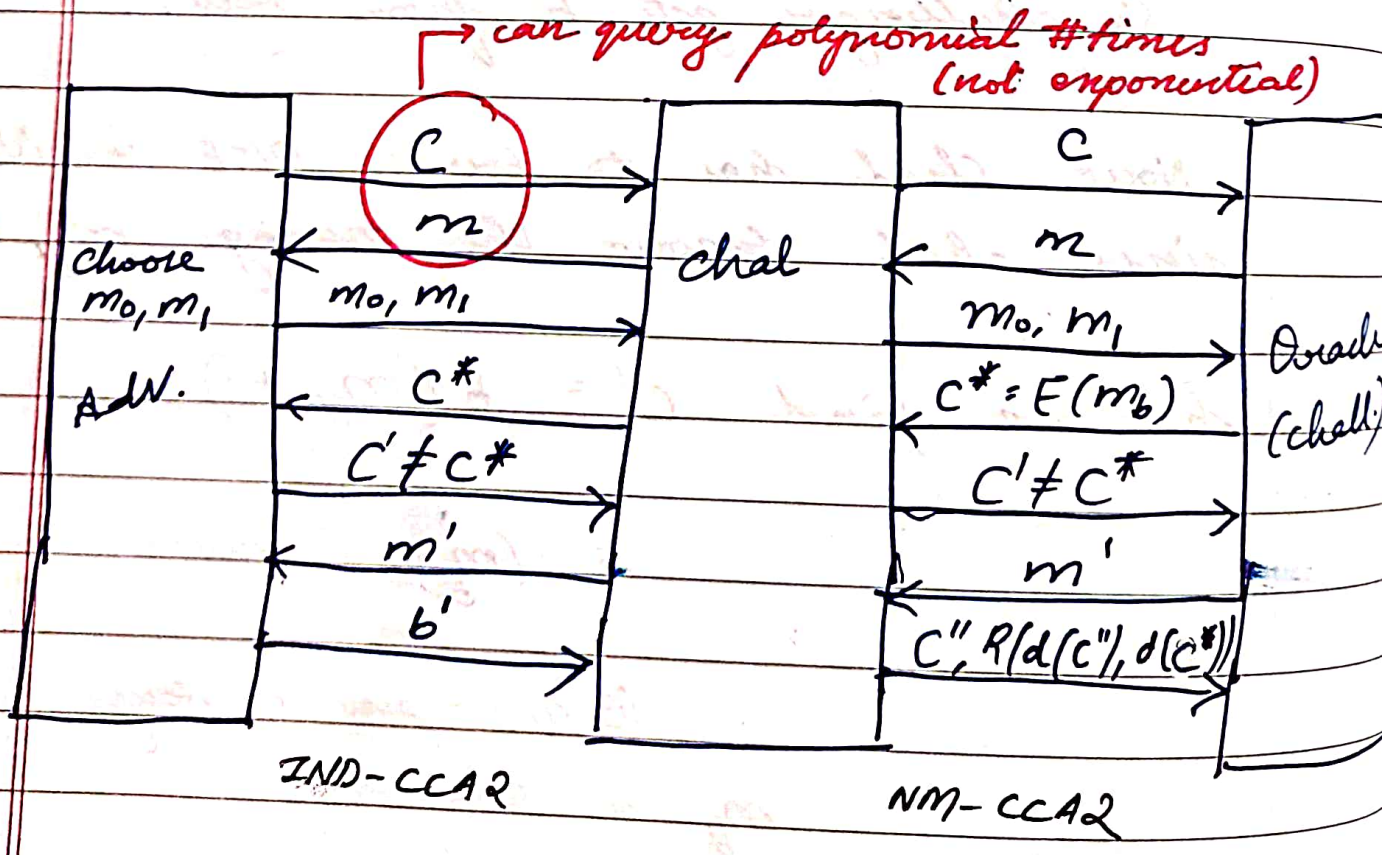
⇒ If PKE is secure in NM-CPA, it is also secure in IND-CPA.

Theorem:

PKE is secure in $\overset{NM}{IND}$-CCA2 if and only if PKE is secure in IND-CCA2

Proof: To prove $A \to B$, we can show $\neg B \to \neg A$ so we prove that

① if PKE is not secure in IND-CCA2, it is also not secure in NMA-CCA2



Adv can break the PKE scheme in IND-CCA2

$\Rightarrow P(b == b') > 1/2$

Now chal. can ~~choose~~ choose

$m'' = m_{b'} + 1$ (since he knows b').

$\therefore C'' = E(m_{b'} + 1)$ $\quad m'' = f(m_{b'}) = m_{b'} + 1$

$= (m_{b'} + 1)^e \bmod n$

(everything is known to calc. to compute C').

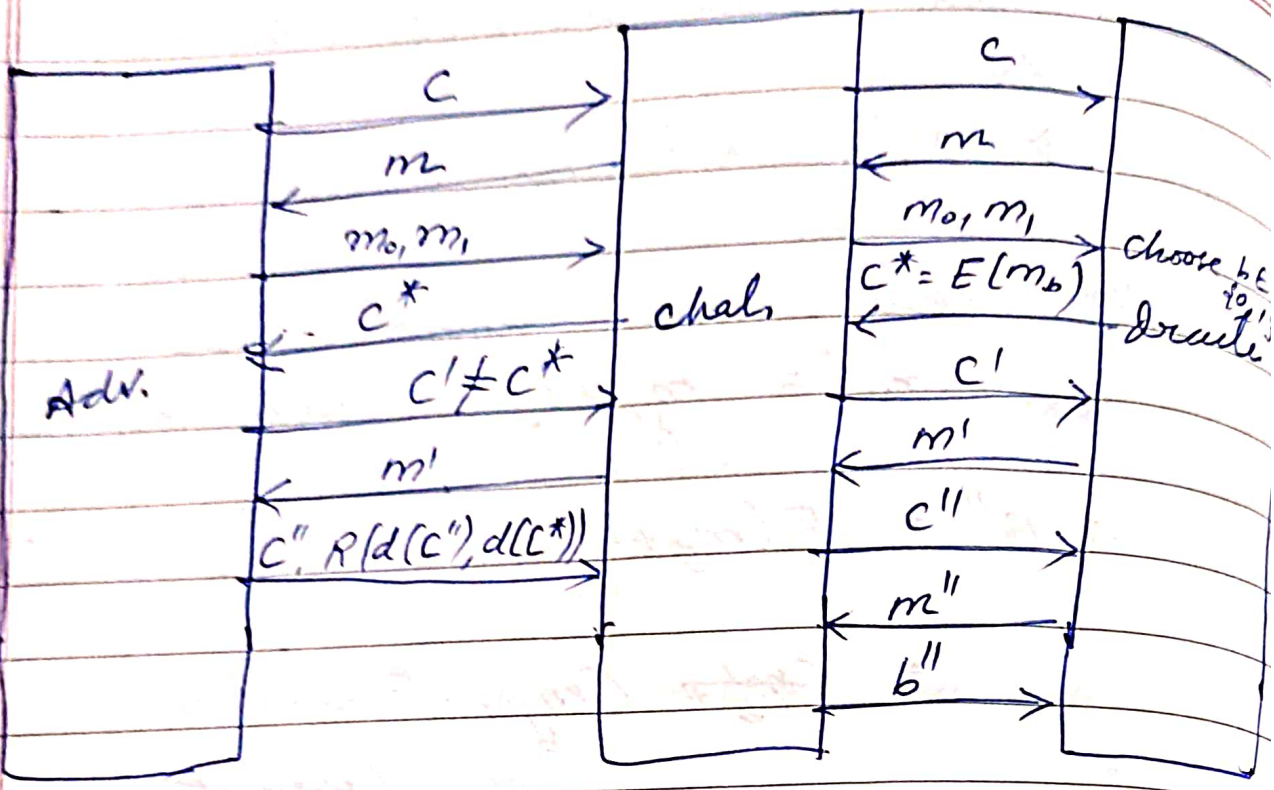
$d(C^*) = m$
$d(C'') = m+1$ } both are related

So adversary can break PKE in NM-CCA2.

26/08/22

(2) IND-CCA2 $\rightarrow$ NM-CCA2

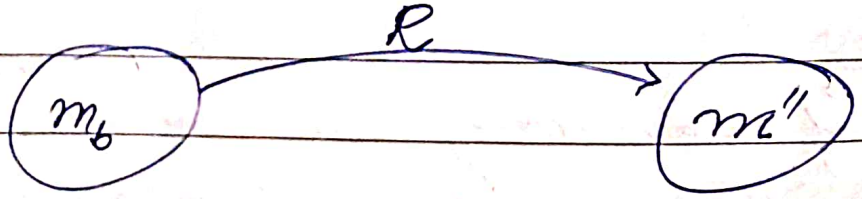
So if adversary can break in NM-CCA2, then there exists another adversary that can break the scheme in IND-CCA2



Adv gives the transformed ciphertext c'' and the relationship between m_b and m''

(chal does not know both m^* and m'' ⇒ he cannot find any one without the other).

So chal queries the oracle for plaintext corresponding to c''.



Now chal knows R and m'', so he

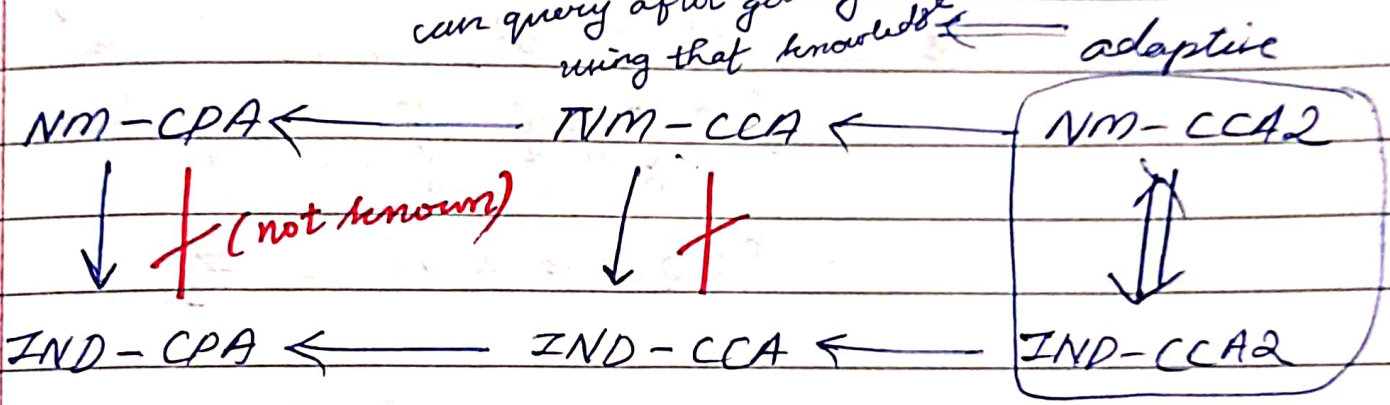
can find m_b

~~Once he~~ if m_b will either be m_0 or m_1

$\Rightarrow$ he can find $b \in \{0,1\}$.

$\therefore P[b'' == b] > 1/2$ since $P[b' == b] > 1/2$

$\therefore$ He can break the scheme in IND-CCA2 also



If scheme is secure is NM-CCA2, then it is also ~~secure~~ secure in NM-CCA

(so NM-CCA $\leftarrow$ NM-CCA2

security of in NM-CCA2 $\Rightarrow$ secure in NM-CCA).

El Gamal

$Z_p = \{1, 2, \ldots, p-1\}$ $*$ mod p forms a group.
(a cyclic group).

(Eg): $Z_7 = \{1, 2, 3, \ldots, 6\}$ $*$ mod 7

Consider 3.

$3 = \{3^1, 3^2, 3^3, \ldots, 3^6\}$ $*$ mod 7

$= \{3, 9, 27, 81, 243, 729\}$

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

$\therefore$ 3 is a generator of Z_7
(5 is also a generator).

Given:

PP: Cyclic group Z_p with generator g

p: 1024 bits (around 5-10 yrs back maybe higher now).

KeyGen(1^n):

Choose $x \in \{2, \ldots, p-2\}$.

$PR = x$ and $PB = g^x \bmod p$

If $x = 1$, $PB = g^x \bmod p = g \bmod p = g$ (useless (no encryption bcos $g \in Z_p$?))

If $x = p-1$

$PB = g^{p-1} \bmod p = 1$ (Fermat's theorem)

So adversary can guess key $= p-1$

$\Rightarrow$ he can find p

$Enc(m, \underbrace{PB_R = y})$: (Randomized encryption)

public key of receiver

Note:

message space $M = Z_p$ $\Rightarrow$ encode msg as $m \in Z_p$.

ciphertext space $C = Z_p$

Choose random number $k \in \{2, \ldots, p-2\}$

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

$Dec(c_1, c_2, x)$:

sender knows $PB_R = y (= g^x \bmod p)$ but does not know $PR_R = x$.

So for sender, computes y^k as $\underbrace{(g^x)^k}$

given without knowledge of x

$\frac{c_2}{c_1} \Rightarrow c_2 c_1^{-1}$

For receiver PR_R : x is known but k is not known

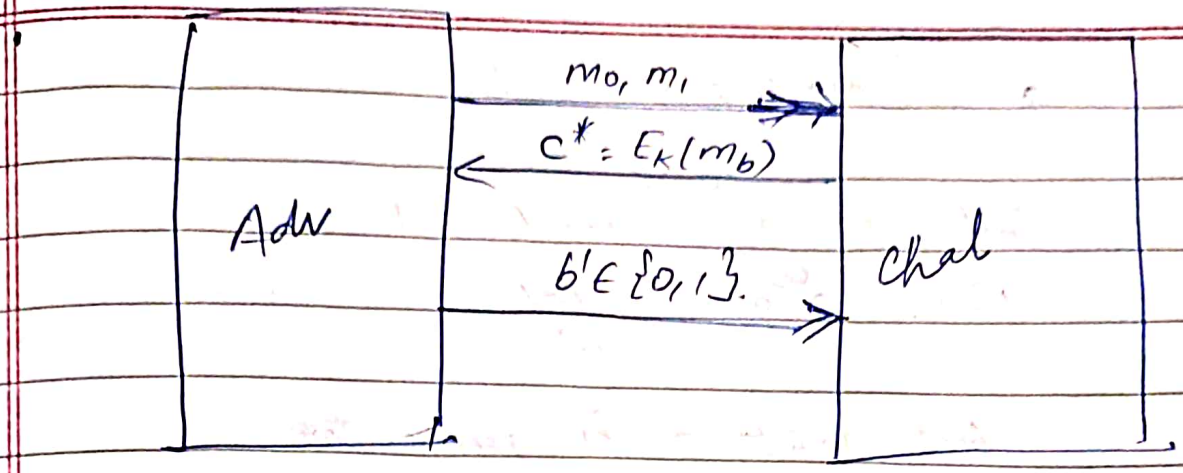
So for him $y^k = (g^x)^k = (g^k)^x$ known to him given to him

$$c_2 = my^k$$
$$= m(g^x)^k$$
$$= m(g^k)^x$$
$$= mc_1^x \quad (c_1 \text{ is } \cancel{\text{given}} \text{ sent to him})$$

$$m = \frac{c_2}{c_1^x}$$
$$= c_2 (c_1^x)^{-1}$$ [this step is implied by $\frac{c_2}{(c_1)^x}$ since we are dealing with g

Theorem :

El Gamal is not IND-CPA secure



To prove: $Adv_{A,\Pi}(n) = P[b == b'] \neq -1/2$

= non negligible

Theorem:

g is QNR mod p.

⇒ There does not exist an x,

such that

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

(Legendre

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

g is generator of cyclic group Z_p.

$$\text{so } g^{(p-1)} \bmod p = 1$$

order $O(g) = p-1$

⇒ $p-1$ is the smallest value for which

$$g^{p-1} \equiv 1 \bmod p.$$

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

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

then $O(g) = \frac{p-1}{2}$

but wkt g is generator

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

which is a contradiction

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

$\Rightarrow$ g is QNR mod p

El Gamal is not IND-CPA secure

Case n: $C_1 = g^k$, $C_2 = my^k$

Case 1: y is QR mod p

$\Rightarrow \left(\frac{y}{p}\right) = 1$.

$\Rightarrow \left(\frac{g^k}{p}\right) = +1$ (or) $y^k = +1$ (??)

$\Rightarrow C_2$ and m share the same property

$C_2 \longleftrightarrow m$

If m is QR mod p then C_2 is QR mod p and vice versa

Choose m_0 = QR(p) and m_1 = QNR(p)

If C_2 is QR(p) $\Rightarrow b = 0$

C_2 is QNR(p) $\Rightarrow b = 1$,

Case 2 : y is QNR mod p.

$$\Rightarrow \left(\frac{y}{p}\right) = -1$$

If k is even, $y^k = 1$.

k is odd, $y^k = -1$.

We need to find the nature of k

Consider $C_1 = g^k$

wkt g is QNR mod p.

If C_1 is QR(p)

then k is even

If C_1 is QNR(p)

then k is odd

i) C_1 is $QR(p)$

$\Rightarrow x$ is even

$\Rightarrow \left(\frac{y^k}{p}\right) = +1.$

$\Rightarrow C_2 \; x \longleftrightarrow m$

If m is $QR(p)$ then C_2 is $QR(p)$

m is $QNR(p)$ then C_2 is $QNR(p)$

choose $m_0 = QR(p)$ and $m_1 = QNR(p)$

If $C_2 = QR(p) \Rightarrow b = 0$

$C_2 = QNR(p) \Rightarrow b = 1.$

ii) C_1 is $QNR(p)$

$\Rightarrow x$ is odd

$$\left(\frac{y^k}{p}\right) = -1$$

$C_2 \longleftrightarrow -m$ &

m is $QR(p) \Rightarrow C_2$ is $QNR(p)$ & vice

choose $m_0 = QR(p)$, & $m_1 = QNR(p)$

C_2 is $QR(p) \Rightarrow b = 1.$

C_2 is $QNR(p) \Rightarrow b = 0$

Problems with El-Gamal:

✓ Dependence on g

$G = g^k$

g is QNR(p)

So if k is even, G is QR(p) and
if k is odd, G is QNR(p).

So for some msgs that are QR(p) & others are QNR(p)

In modified El-Gamal, we replace g with QR(p)

⇒ all msgs and ciphertexts are QR(p)

Theorem:

* El-Gamal is not IND-CCA secure

*. El-Gamal is malleable

Schnorr Group :

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

$g = 3$

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

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

$G = \{2, 4, 1\} = \{2^1, 2^2, 2^3\} \pmod 7$

$\Rightarrow$ a cyclic sub-group of Z_7 (Schnorr group).

elements is prime $\left(= \frac{7-1}{2} = 3\right)$.

Choose primes p, q such that $(p-1) = 2q$

Cyclic subgroup of Z_p of order q is called Schnorr group.

Consider cyclic group Z_p with generator h

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

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

Let $g = h^2$

Consider cyclic group G with generator g

h is ~~QR~~ QNR mod p

$g = h^2$ is QR mod p.

Modified El-Gamal

pp: cyclic group G with generator g.

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

g is QR mod (p)

$\Rightarrow$ m is QR mod p

c is QR mod p.

Key Gen (1^n) :

Choose $x \in \{G - 1\}$ (exclude 1)

$PR = x \qquad PB = g^x$

Enc $(m, PB_R = y)$:

Choose $k \in \{2, \ldots, p-2\}$ randomly

$c_1 = g^k \;,\; c_2 = m y^k$

Dec (c_1, c_2, x) :

$$m = \frac{c_2}{c_1^x} = c_2 (c_1^x)^{-1}$$

Both (original & modified).

Theorem:

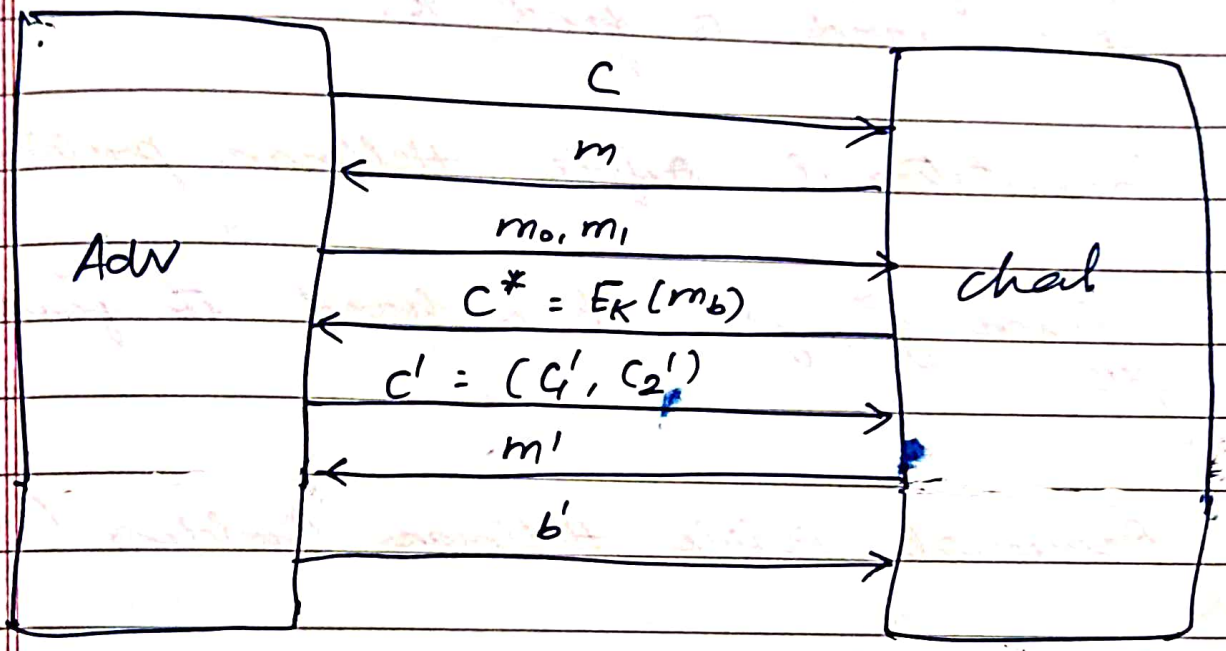
El Gamal is not CCA secure

$C_1^* = g^k$ $\quad C_2^* = my^k$

$C^* = (C_1, C_2)$. is known

Let $C_1' = g^k$, $\quad C_2' = rmy^k = rC_2^*$

⇒ Adv gets rm back from challenger



Adv knows r and $rm = m'$.

$\therefore \quad m' = rm$

~~$m = r^{-1}b'$~~

$m = \frac{m'}{r} = r^{-1}m'$ (both known)

HW El Gamal is malleable

29/08/22

* Hard Problems in El Gamal

~~For any cyclic group given g, given $g, g^x \bmod p$ and g, it is difficult/hard to find x~~

1. Discrete logarithm problem (DLP):

In any cyclic group, given g and $y = g^x \bmod p$, it is hard to find x

2. Computational Diffie Hellman problem (CDH)

Given g^x, g^y, it is hard to find g^{xy}

3. Decisional Diffie Hellman Problem (DDH)

Easy in elliptic groups

Hard in certain groups like Schnorr groups

$Z_7 = \{1, 2, \ldots, 6\}$

$h = 3$

$g = h^2 = 9 \equiv 2 \pmod 7$

$\therefore G_1 = \{2^1, 2^2, 2^3\}$ $\left(O(G_1) = \frac{p-1}{2}\right)$

$= \{2, 4, 1\}$ $p = 7$

$\hookrightarrow 8 \bmod 7$

Schnorr group.

DDH is hard in G but not in Z_p.

↓

cyclic subgroup of Z_p (schnorr group),

DDH Problem:

Given g^x, g^y, g^z

find whether $z = xy$ or not is hard

⇒ Depends on CDH problem

(if we can find g^{xy} from g^x, g^y we can easily check whether $z = xy$ or not).

Theorem:

Modified El Gamal is IND-CPA (semantically) secure

If adversary can break our scheme (with non-negligible probability in feasible time) then (i) there exists another adv. who can break the proved scheme (from which our scheme is derived) ~~in~~ with non-negligible probability in polynomial time (or) (ii) there exists another adv who can solve the hard problems with non-negligible probability in polynomial time

↓ implied by 'can break'

$A \rightarrow B$

A ↓ can break our scheme

B ↓ can break proved scheme (or) can solve hard problems

If $A \rightarrow B$ then $\neg B \rightarrow \neg A$

i.e security of proved scheme implies / guarantees security of our scheme

wkt B is F (cannot break proved scheme).

$\Rightarrow \neg B$ is T.

wkt ~~$\neg B \rightarrow \neg A$~~ is T.

$A \rightarrow B$ is T.

B is F

$\Rightarrow$ A is F

i.e ~~one~~ cannot break our scheme

(or) our scheme is secure

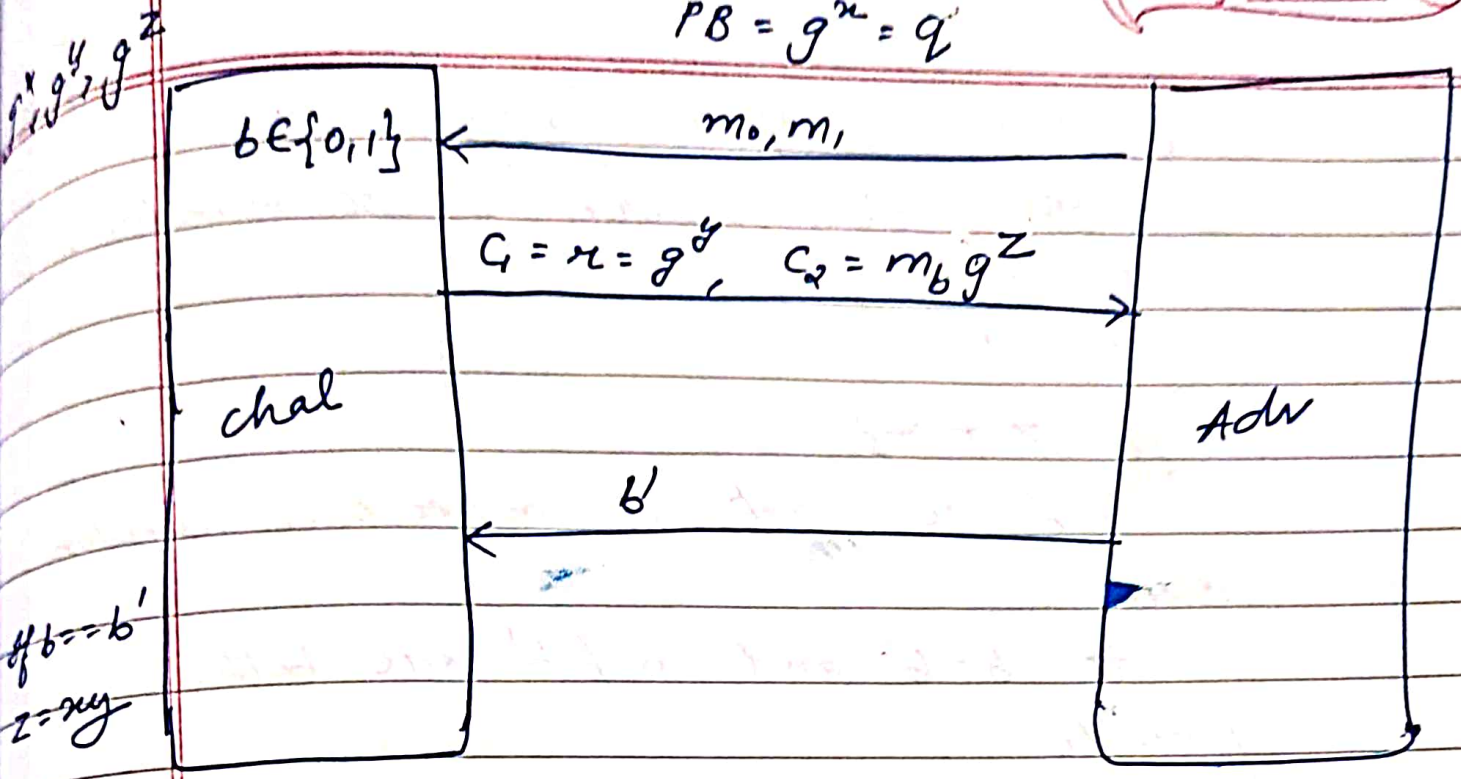
Consider the hard problem given g^x, g^y, g^z find whether $z = xy$ or not.

Chal has to solve this problem using the Adv's ability

challenger has to give the valid public parameters to the Adv

→ one that he has to be broken to break the scheme

Let us say $PB = g^x$ ($CA = g^x$ is public)



$PB = g^x$

$c_1 = g^t$, $c_2 = m(PB)^t$

~~if $t = y$~~ If $t = y$

$c_1 = g^y$, $c_2 = m(g^x)^y$

$= m(g^{xy})$

so if we send $c_2' = m(g^z)$, then if $z = xy$, $c_2 = c_2'$

if $b \neq b'$, then $z \neq xy$

$\Rightarrow$ ~~then~~ the answer ~~b'~~ is random

So $Pr(b = b')$ is

if $z \neq xy$

b' we get is ~~a~~ like random value

$\Rightarrow$ $b = b'$ and $b \neq b'$ are both possible

so if $b \neq b'$,

Chal can be sure $z \neq xy$

if $b == b'$

chal can guess ~~$z \neq$~~ $z = xy$ with non-negligible prob.

In El-Gamal

$C_1 = g^k$, $C_2 = m(PB)^k$

if $PB = g^x$ and $C_1 = g^y$

$C_1 = g^y$, $C_2 = m(g^x)^y$

$= m g^{xy}$.

Adv can break my scheme

$\Rightarrow$ Given above C_1, C_2, he can find

m

Let us send

$c_1' = g^y$ and $c_2' = m_b g^z$

If $z = xy$

the encryptions c_1, c_2 correspond to El-Gamal on m_b and adv can find m_b ⇒ he predicts $b' = b$ with prob. 1.

If $z \neq xy$,

encryption to c_1, c_2 is not the $Enc(m_b)$ using El-Gamal

⇒ adv would find $m' \neq m$

01/09/22

Field:

→ Tantamount to 2 groups

Field → $F, \oplus, \circledast$

set F and the 2 ~~above~~ operations $\oplus$ $\circledast$ forms a field if it satisfies the following properties:

$F, \oplus$ forms a commutative group. (Abelian group).

1. Closure: $\forall a, b \in F$
$a \oplus b \in F$

2. Associativity: $\forall a, b, c \in F$
$(a \oplus b) \oplus c = a \oplus (b \oplus c)$

3. Identity: $\exists e \in F$ such that
$a \oplus e = e \oplus a = a$

4. Inverse: (Additive). $\forall a \in F$, $\exists a^{-1} \in F$ such that $a \oplus a^{-1} = a^{-1} \oplus a = e$

5. Commutativity: $\forall a, b \in F$
$a \oplus b = b \oplus a$

$F, \circledast$

6. Closure : $\forall a, b \in F$

$a \circledast b \in F$

7. Associativity : $\forall a, b, c \in F$

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

8. Identity : $\exists\ e' \in F$ such that
(Multiplicative) $a \circledast e' = a$

9. Inverse : $\forall\ a \in F - \{e\}$ (e → additive identity)

~~$a \cdot a^{-1}$~~ $a \circledast a^{-1} = e'$

(all elements except additive identity e have multiplicative inverse)

10. Commutativity : $a \circledast b = b \circledast a$

$\forall a, b \in F$

11. Distributive : $\forall a, b, c \in F$

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

(only second operation over first operation)

→ used in crypto (finite field)

(Eg): 1) $Z_p = \{0, 1, 2, \ldots, p-1\}$, +, × mod p.

~~$(Z_p, +)$ → closure ✓~~

$(Z_p, +\bmod p)$ → closure ✓
associativity ✓
identity ✓ $(e = 0)$
inverse ✓ $(a^{-1} = p - a)$.
commutativity ✓
⇒ abelian group

$(Z_p, \times \bmod p)$ → NOT an abelian group
(0 does not have inverse).
closure ✓
associativity ✓
identity ✓ $(e' = 1)$
inverse ✓ $(a^{-1} = a' \bmod p$
except for $a = 0$).
commutativity ✓

Distributivity : $a \times (b + c) = a \times b + a \times c$ ✓

⇒ Z_p, +, × mod p is a field

size of R

2) $(R, +, \times)$ → infinite field (not used in crypto)

$(R, +)$ → abelian group

$e = 0$

$(R, \times)$ → not a group (no inverse for 0).

$(R-0, \times)$ → group.

distributivity ✓

⇒ It is a field

* Smallest field :

$Z_2 = \{0, 1\}$, + mod 2, × mod 2

In a computer, if we use n bits, we have 2^n possible bit combinations

If we use m bits ~~for~~ to represent p, then generally

$p \ll 2^m$ (extra, unused bit combinations are possible)

so ~~if~~ we look at field of size 2^n

3) $(C, +, \times)$ → also a field

(For multiplicative inverse ⇒ $\frac{1}{a+ib} = \frac{a-ib}{a^2+b^2}$)

*. prime polynomial
⇒ by default - over the field of real numbers.
⇒ like prime numbers, prime poly. cannot be factorized (has only 2 factors 1 and itself).

(Eg): x^2+1 ⇒ pp over field of real nos but not pp over field of $\mathbb{C}$
$[x^2+1 = (x-i)(x+i)]$.

Theorem:
Prime polynomials exist for every possible degree.

*. Field (2^n) : ← size

$F = \{ a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1 x + a_0 \}$ (all poly of degree $< n$)

size of F is 2^n

$\forall i,\ a_i \in \mathbb{Z}_2$

pp = prime polynomial of degree n
⇒ F_1 + mod pp, × mod pp is a field (of size 2^n).

$|F| = 2^n$

$(F, +_{mod\ pp})$

Closure : $1+x+x^2, \quad x+x^2$

$$\begin{array}{r} 1+x+x^2 \\ + \quad x+x^2 \\ \hline 1+(1+1)x+(1+1)x^2 \end{array}$$

$\Downarrow$

$1+1 \neq 2$ (this addition is over the field of real nos, not $\mathbb{Z}_2$)

whenever we deal with elements of a field, we can only apply the operations of the field

Associativity : ✓

Identity : $0 \in F$ ✓

Inverse : $f^{-1}(x) = f(x)$ ✓

(when you do ~~+mod~~ $f +_{mod_2} f$, you get $0 = e$).

Commutativity ✓

$(F, \times \bmod 2)$

Closure ✓

Associativity ✓

Identity : $1 \in F$ ✓

~~Inverse~~

Inverse :

Use Extended Euclidean Algo

$\forall f(x) \in F,$

$\gcd(f, PP) = 1$ bcos pp is prime poly

$\Rightarrow af + b(pp) = 1$

and a, b exist ~~where~~

$\Rightarrow a = f^{-1} \bmod pp$ exists ✓

Commutativity ✓

Distributivity ✓

$\therefore (F, +_2, \times_2)$ is a field

Theorem:

Given x, y, $\exists a, b$ such that

$ax + by = GCD(x, y)$.

(Ex): $x = 18, \quad y = 12$

		q	x_x	x_y
x	18		1	0
y	12	18/12 = 1	0	1
18%12 =	6	12/6 = 2	1 - 1.0 = 1	0 - 1.1 = -1
12%6 =	0			6
	stop			

(previous-to-previous value − quotient * previous value)

$1 \times 18 + (-1) \times 12 = GCD(18, 12)$

$= 6$

$x = 18, \quad y = 13.$

		q	x_x	x_y
	18		1	0
	13	18/13 = 1	0	1
18%13	5	13/5 = 2	+1	-1
13%5	3	5/3 = 1	-2	3.

		3	-4.
2	1		
1	2	-5	7.
0			

$-5(18) + 7(13) = GCD(18, 13) = 1$

$-90 + 91 = 1$

02/09/22 $28^{-1} \bmod 75$

$x = 75, \quad y = 28$

$GCD(75, 28) = 1$

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

	q	r_x	r_y
75		1	0
28	2	0	1
19	1	1	-2
9	2	-1	3.
1	9	3	-8
0			

$28^{-1} \bmod 75 = -8$

$\equiv \cancel{-(75-8) \bmod 75}$

$= 67 \pmod{75}$

$(67-75) \bmod 75$

$\equiv 67 - 0$

$\equiv 67$

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

or

$3 \times 75 + 67 \times 28 \equiv 1 \pmod{75}$.

$ax + by = 1$

$\Rightarrow ax + by \equiv 1 \pmod{x}$

$axy^{-1} + byy^{-1} \equiv y^{-1} \bmod x$

$(ay^{-1}.x) \bmod x + b.\bmod x = y^{-1} \bmod x$

$(kx \bmod x = 0)$ $\quad b = y^{-1} \bmod x.$

$[axx^{-1} + byx^{-1} = x^{-1}] \bmod y$

$(ky \bmod y = 0)$

$a \bmod y + bx^{-1}y \pmod y = x^{-1} \bmod y$

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

Complexity of Extended Euclidean Algo is $O(\log n)$.

$b = 1 - (x+3)(4x+1)$

$= 1 - [4x^2 + 13x + 3]$

$= x^2 + 2x + 3 \quad 1 - [4x^2 + 3x + 3]$

$= 1 + x^2 + 2x + 2 \quad = x^2 + 2x + 3.$

$a = x + 4, \qquad b = x^2 + 2x + 3$

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

$= x + 4. \qquad = x^2 + 2x + 3.$

(b/cos GCD = 1),

↳ so inverse exists

Characteristic number of a field

⇒ The number of times multiplicative identity must be added to get the additive is identity.

(Eg): 1. Field (Z_2)

$AI = 0$

$MI = 1$

2 times

$\Rightarrow 1 + 1 = 0$

Char. no = 2

2. Field (p)

$AI = 0$

$MI = 1$

$\Rightarrow$ char no = p.

3. Field (2^p).

$AI = (0, 0, 0, \ldots, 0)$

$MI = (0, 0, 0, \ldots, 1)$

$$\begin{array}{r} (0,0,0,\ldots,1) \\ +(0,0,0,\ldots,1) \\ \hline (0,0,0,\ldots,0) \end{array}$$

↳ because $q_0 \in Z_2$

$\therefore$ char. no = 2

4. Field ($\mathbb{R}$) ← real numbers

char no = 0 (no way of adding 1 to get 0 back $\Rightarrow$ no mod operation work)

~~Ho Ho~~ Intuition :

(char no. $\otimes$ MI) $\equiv$ AI

↓

normally normal multiplication for real no.

$\times \bmod p$ for field ($\mathbb{Z}_p$)

Elliptic curve (cubic equation)

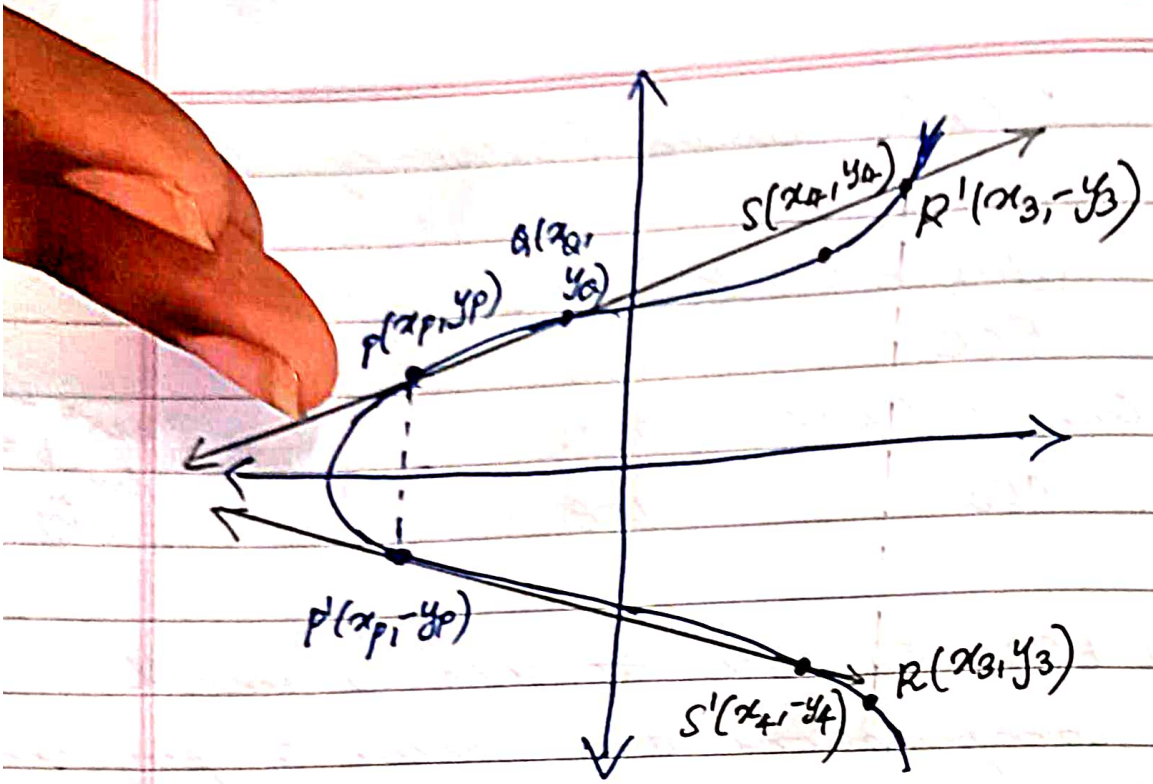
Scheme	Key size	
ECC	256	all 3 give the same level of security
ElGamal / RSA	3072	
AES	128	

In ECC, the key ~~is~~ size is small so computations are easier to perform
$\Rightarrow$ ECC is much more efficient than ElGamal / RSA
ECC is an example of light-weight cryptography

AES → even smaller key size
Any symmetric system like AES is much more efficient than any other public key cryptography

~~ECC $\Rightarrow$ only~~

If char. no. $\neq 2$
$y^2 = x^3 + ax + b$ is the elliptic curve
(symmetric about



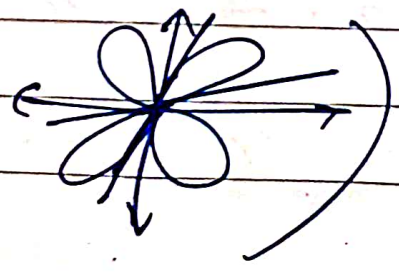
9/22 Non-singular Elliptic Curve over the field $\mathbb{Z}_p$

Assuming $p > 2$ $(p \neq 2)$.
(Can be over field of Real nos as well).
↳ instead of $\mathbb{Z}$

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

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

(singular - different ~~tg~~ tangents are possible at one point?
⇒ not very secure



For ~~non~~ non-singular curves:

$$4a^3 + 4 2 b^2 \neq 0 \quad \rightarrow (= 0 \text{ for singular})$$

(For singular curves

$$\frac{df}{dx} = 0, \quad \frac{df}{dy} = 0, \quad \frac{d^2f}{dx\,dy} = 0$$

$\Rightarrow$ solve them to get the above eqn).

ECC & El-Gamal are same but only the ~~gr~~ group is different.

$E_{a,b} = \{$ points on the elliptic curve, ∞ (point at infinity) $\}$, $\oplus$

$\downarrow$

not infinity - It is an imaginary point

definition of $\oplus$ operation:

Case 1: $P(x_p, y_p) \oplus \infty = P(x_p, y_p)$

(1 point is point at infinity) Illy $\infty \oplus P(x_p, y_p) = P(x_p, y_p)$.

Case 2: $P(x_p, y_p) \oplus P'(x_p, -y_p) = \infty$

(conjugate points same x, negated y)

Case 3: (2 different points such that $x_1 \neq x_2$).

Consider 2 points $P(x_P, y_P)$ and $Q(x_Q, y_Q)$ such that $x_P \neq x_Q$

Now draw a line joining these 2 points and find the 3rd point R' where the line intersects the curve again.

Now find the conjugate of $R' = R(x_3, y_3)$. [R' is $(x_3, -y_3)$].

Equation of PQ be $y = mx + c$

$$m = \frac{y_Q - y_P}{x_Q - x_P} = \frac{y_2 - y_1}{x_2 - x_1}$$

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

$\Rightarrow (mx+c)^2 = x^3 + ax + b$

$x^3 - m^2x^2 + \square x + \square$

If x_1, x_2, x_3 are roots then

$$x_1 + x_2 + x_3 = -\frac{(-m^2)}{1}$$

$$= m^2$$

we known x_1, x_2 and hence we can find x_3.

$$x_3 = m^2 - x_1 - x_2$$

wkt m = slope of PQ

= slope of PR'

$$= \frac{y_3 - y_1}{x_3 - x_1}$$

$$y_3 = m(x_3 - x_1) + y_1$$

Using x_3, we can find y_3.

Case 4: $P = Q$.

Draw a tangent at P'

It intersects the curve at $S'(x_4, -y_4)$

Consider its conjugate $S(x_4, y_4)$.

Eqn of tgt is $y = mx + c$

$$m = \frac{\partial y}{\partial x}\Big|_P$$

$$= \frac{\partial}{\partial x}(x^3 + ax + b)$$

$$= \frac{3x_p^2 + a}{2y_p}.$$

$$y^2 = x^3 + ax + b$$
$$2y\,dy = 3x^2\,dx + a\,dx$$
$$\frac{dy}{dx} = \frac{3x^2 + a}{2y}$$

Theorem:

$(E_{a,b}, \oplus)$ forms a group

Proof:

Closure: $\oplus$ always gives a point on the curve (∞ or intersection of tgts on the curve and their conjugates are only the points we deal with).

↓

all of which are on the curve

Associativity: (Assume).

Identity: ∞

$(P \oplus \infty = \infty \oplus P = P)$

Inverse : conjugate

$P \oplus P' = \infty$

So inverse of $P(x, y) = P'(x, -y)$.

If x and $y \in Z_p$

$\Rightarrow$ max. no. of points $= p^2$

but many points will not be on the curve

p should be sufficiently large to prevent brute force attacks.

1. Let $a = 1$, $b = 6$, field be Z_7 Z_5

$y^2 = x^3 + x + 6$.

Find $E_{1,6}$

$x = 0$

$y^2 = 6 \pmod{5}$

$\equiv 1 \pmod 5$ bcos field is Z_5.

$y = 1, 4$

$\hookrightarrow p - 1 = 5 - 1$ is also a soln.

Points are $(0, 1), (0, 4)$

$x = 1$

$y^2 = 1+1+6 = 8$

$\equiv 3 \pmod 5$.

$3^{\frac{(5-1)}{2}} = 3^2 = 9 \not\equiv 1 \pmod 5$

$\therefore$ 3 is QNR mod 5

$\Rightarrow$ no soln.

$x = 2$

$y^2 = 8+2+6$

$= 16$

$\equiv 1 \pmod 5$.

$y = 1, 4$.

Points are $(2,1), (2,4)$

$x = 3$

$y^2 = 27+3+6$

$= 36$

$\equiv 1 \pmod 5$

$y = 1, 4$

Points are $(3,1), (3,4)$.

$x = 4$

$$y^2 = 64 + 4 + 6$$
$$= 74$$
$$\equiv 4 \pmod 5$$

$y = 2, 3.$

$\therefore$ Points are $(4,2)$, $(4,3)$.

$\Rightarrow$ Totally only $8 + 1$ (for ∞) $= 9$ points (not $5 \times 5 = 25$).

$$E_{1,6} = \{(0,1), (0,4), (2,1), (2,4), (3,0), (3,4), (4,2), (4,3), \infty\}.$$

$\Rightarrow$ This may or may not be a cyclic group

But there always exists a cyclic sub-group which is used as the message space & cipher-text space in ECC