Sunil
DATE
PAGE
"Rough 'n' Fair"

Cryptography

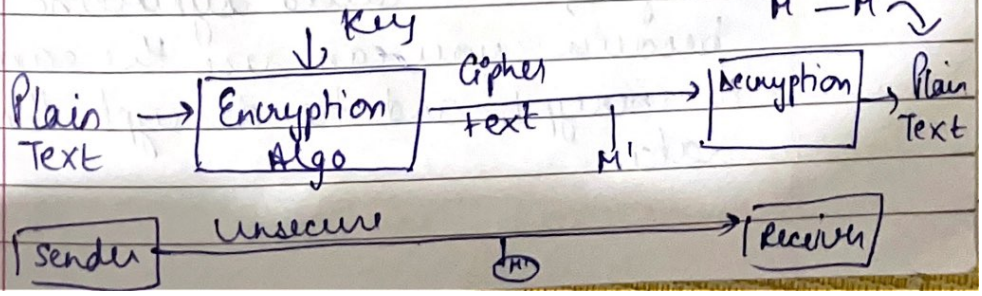
Cryptography is the study of secure communication techniques that allow only the sender and intended recipient of a message to view its contents.
The term is derived from the greek word Kryptos which means hidden

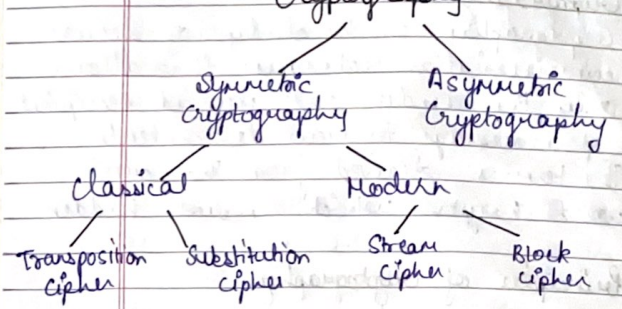
Principles of Cryptography

1) Confidentially: It refers to certain rules and guidelines usually executed under confidentially agreements which ensure that the information is restricted to certain people or places

2) Data Integrity: It refers to maintaining and making sure that the data stays accurate and consistent over its entire life cycle.

3) Authentication: It is the process of making sure that the piece of data being claimed by the user belongs to it.





Assymmetric Key Cryptography / Public Key Cryptography
It is a cryptographic system that uses pairs of keys. The generation of such key pairs depend on cryptographic algorithms which are based on mathematical problems termed one-way functions

Symmetric Key Cryptography / Secret Key Cryptography
It is the use of a single based shared secret to share encrypted data between parties. Ciphers in this category are called symmetric because you can use the same key to encrypt and to decrypt the data.

Attacks is a method for circumventing the security of a cryptographic system by finding a weakness in a code, cipher, cryptographic protocol or key management scheme. Attacks are typically categorized based on the action performed by the attacker. An attacker, there can be passive or active

- In an active attack, an attacker tries to modify the content of the messages
- In a passive attack, an attackers observes the messages and copies them.

Encryption is the process of translating plain text data into something that appears to be random and meaningless (cipher text)

Decryption is the process of converting cipher text back to plain text.

Cipher is an algorithm for performing encryption or decryption - a series of well defined steps that can be followed as a procedure
A cipher converts the original message called plaintext into cipher text using a key to determine how it is done.

Block Cipher	Stream Ciphers
It converts the plain text by taking each block individually	It converts the plain text by taking one byte of the plaintext at a time.
Uses either 64 bits or more than 64 bits	uses 8 bits
Complexity is simple	More complex
Uses confusion as well as diffusion	uses only confusion
Reverse encrypted text is hard	Reverse encrypted text is easy
It is slow	It is fast
Algorithm used are ECB (Electronic Code Block) CBC (Cipher Block Chaining)	Algorithm used are CFB (Cipher Feedback) OFB (Output Feedback)

Bit	Byte
Smallest unit of computer information. It's essentially a single binary data point, either yes or no on or off, up or down	Unit of memory that usually contains 8 bit. This is because historically, 8 bits are needed to encode a single character of text

Cryptography is the science of writing in secret code so that no other person except the intent receipt could read.

Crypto means hidden secret and graphic means to write or study

Cryptography is the practice and study of technique for secure communication in the presence of third party.

More generally it is about constructing and analysing protocols that overcome the influence of attacker or outside people and which are related to various aspect in information security such as data confidentiality, data integrity, authentication.

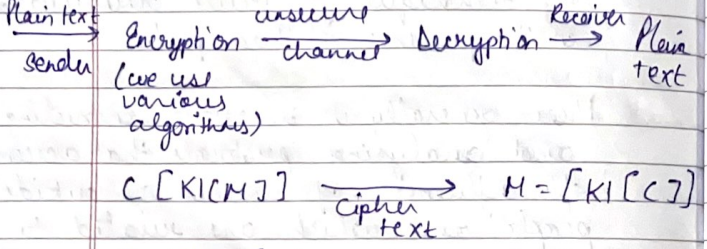
Applications of Cryptography
It includes ATM cards, computer passwords, etc.

It is the science of using mathematic to encrypt or decrypt the data. It enables you to store sensitive info or transmit it across insecure channel (network)

Types of Cryptography

1) Symmetric Key Cryptography (same Key) Private / Secret Key Cryptography

Key methods - DES, 3DES, AES

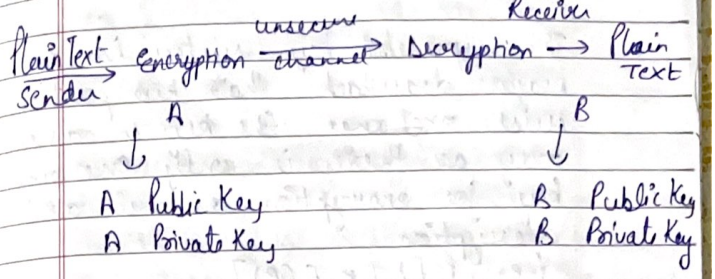


C [KI[M]] → (Cipher text) → M = [KI[C]]

C = Cipher Text
KI = Key
M = Message (Plain Text)

public Key is broadcast at any point of time

2) Assymetric Key Cryptography (public Key Cryptography)



Cases
1) A = E [A Public Key [M]] send to B ✗
2) A = E [B Private Key [M]] send to B
3) A = E [A Private Key [M]] send to B ✗

→ confidentiality not achieved

4) A = E [B Public Key [M]] send to B ✓

Always use receiver public key to encrypt the message.

Symmetric Key Cryptography
Also known as private Key / secret Key cryptography

In symmetric key cryptography a single key is used for both encryption & decryption

AES (Advanced Encryption System) most widely used symmetric key cryptography (AES, 2DES, 3DES)

The symmetric key system has one major drawback that two parties must exchange the key in a secure way as there is only one single key for encryption as well as decryption
i.e $P = [D(K, E(P))]$
where K - Key for both (encryption & decryption)

P = Plain Text
D = Decryption
E(P) = Encryption for Plain Text

Stenography
The action or process of writing in shorthand and transcribing the shorthand on a typewriter

Advantages of Symmetric
- It is faster
- encrypted data can be transferred on the link even if there is a possibility that the data will be intercepted since there is no key transmitted with the data, the chances of data being decrypted are null.
- A symmetric uses password authentication to prove the receivers identity.
- A system only which possesses the secret key can decrypt a message.

Disadvantages of Symmetric
- Have a problem of Key transportation The secret key is to be transmitted to the receiving system before the actual message is to be transmitted. Every means of electronic communication is insecure ~~of~~ as it is impossible to guarantee that no one will be able to tap communication channels. So the only secure way of exchanging keys would be exchanging them personally.
- cannot provide digital signatures that cannot be repudiated.

Advantages of Assymmetric
- In this, there is no need for exchanging keys, thus eliminating the key distribution problem
- Increased security: the private key do

not ever need to be transmitted or revealed to anyone
- can provide digital signatures that can be repudiated.

Disadvantages of Asymmetric
for encrypting this method is slow
there are popular secured-key encryption methods which are significantly faster than any currently available public-key encryption method.

Security Services
Confidentiality
integrity
Authentication → (password)
Non-repudation → (proof of access)
Access control

Asymmetric Key Cryptography
Also known as public key or conventional cryptography

In this two keys are used for encryption and decryption
$P = D(K_d, E(K_e, P))$

Cryptosystem
A system which converts plain text to cipher text by the application of encryption or decryption algorithms

The key generation for encryption & decryption algorithm is also a part of a cryptosystem

A cryptosystem is an implementation of cryptographic techniques

Plain Text → Encryption → Cipher → Decryption → Plain Text
(Sender) algorithm + Key → unsecure channel → 'Key' (Receiver)

Plain Text : This is the data that needs to be protected

Encryption Algorithm : This is the mathematical algorithms that takes plain text as the input and return cipher text.
It also produce the unique encryption key for the text.

Cipher Text : This is the encrypted or

unreadable form of the plain text

Decryption Algorithm: This is the mathematical algorithm that takes cipher text as the input and decode it into plain text or original text

It also use the unique decryption key for the text.

Encryption Key: This is the value known to the sender that is used to compute the cipher text for the given plain text

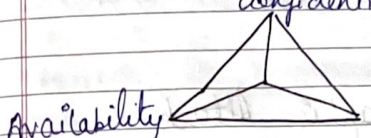
Decryption Key: This is the key known to the receiver that is used to decode the given cipher text to plain text.

Challenges of Symmetric Key Cryptography

1) **Key Establishment:** Before any communication both the sender and the receiver needs to agree on a secret symmetric key.

2) **Trust Issue:** Since the sender and the receiver use the same symmetric key, there is an implicit requirement that the sender and the receiver trust each other.

Security Goals - CCIA Triads in Cryptography



Confidentionality (privacy)

- It is the most common aspect of information security.
- It allow authorised users to access sensitive and protected data. The data sent over the network should not be accessed by unauthorized user.
- Attackers will try to capture the data so to avoid this various encryption techniques are used to save our data so that even if attacker gain access the and she will not be able to decrypt it.

Integrity

means that changes need to be done

Information is useless if we cannot access it what would happen if we cannot access our bank Account for transaction?

by the authorized entity and through authorised Mechanisms. and nobody else should modify our data.

Availability
Data must be available to the authorized user.

Cryptographic Attack

Cryptoanalytic Attack

eg (Brutoforce attack)
tools → Hydra, Crack
Hacking small passwords

(Dictionary attack)
Hacking long length passwords

Non-Cryptoanalytic Attack

eg (Security attack)
↳ security attack
↳ security Mechanism
↳ security services
⇓
applied on CIA
↙ ↘
passive active

Attacks

Attack is any attempt to explore, alter, destroy, steal or gain information through unauthorized access

Bruteforce attack
It uses trial and error to guess logging information, encryption Key, or find a hidden web page
eg - crack, hydra, rainbow crack etc

Security Dictionary attack
It is a password-guessing technique by trying many common words and their simple variations. Attackers use extensive lists of the most commonly used passwords, popular pet names, literally just words from a dictionary

Security Attack. (RFC (Request for comment))
OSI security model focus on three basic aspect of network security.

a) security attack
b) security Mechanism
c) security services

Three goals of security (CIA) can be threaten by security attacks.

Security Attack
- Threat of confidentiality
- Threat of Integrity
- Threat of availability

Sunil
DATE
PAGE
"Rough 'n' Fair"

Threat of Confidentionality
→ Snooping
→ Traffic analysis

Snooping: It is unauthorized access to data or information

Traffic analysis: we encrypt the information, so that the attacker even if captured the message, could not extract any information from the message.
eg → net flow analyser
Microsoft message analyser

Threat to Integrity
→ Modification
→ Masquerading attack
→ Replay attack
→ Repudiation

Modification
After accessing the information the attacker after the message or that message could be delayed or delete. done by unauthorized user.

Sunil
DATE
PAGE
"Rough 'n' Fair"

Masquerading attack (spoofing)
It happen when the attacker impersonate somebody else i.e one entity pretend to be a different entity.
eg → a user try to contact a bank but another site pretend that it is the bank and obtained info.

Replay attack (playback attack)
The attacker obtained a copy of a message send by a user and later try to replay or resend or delay it.
eg → text dependent speaker verification.

Repudiation
It can be done by the sender or receiver. The sender of the message might later deny that he has sent the message, the receiver might later deny that he has receive the message

Threat of Availability

Denial of services (DOS)
An attempt to make a server or

Machine or network resources unavailable to its intent users.

Security Attack
→ Passive
→ Active

Passive Attack
It attempt to learn or make use of the information from the system but does not affect the system resources i.e the attacker will only see the data, he will not modify it.

To prevent, we can prevent it using encryption techniques

Types of Passive attacks

1) Release of message content
Eg- Bruteforce attack
The attacker will easily able to understand the data or information

2) Traffic Analysis
If we have encryption protection and attacker might still be able to see the pattern of these messages

The attacker could determine the location and identify of communication host and could observe the frequency and length of the message being exchanged

Active Attack
Active attack - it attempt to alter the system resource and information
It involve some modification of data stream or creation of false statement.

Caesar cipher Encryption
$E_M(x) = (x+K) \text{ Mod } M$
- x → value of particular letter
- K → Key
- M → Modulus → Max limit of set

Zayn will sing a song Key = 7
Gh fyl dpss zpyn h zvyn

1) $= (25+7) \text{ Mod } 26$ (z)
$= 32 \text{ Mod } 26$
$= 6$ (g)

2) $= (0+7) \text{ Mod } 26$ (a)
$= 7$ (h)

3) $= (24+7) \text{ Mod } 26$ (y)
$= 5$ (f)

4) = (18+7) Mod 26 (n)
= 25 (u)

5) = (22+7) Mod 26 (w)
= 3 (d)

6) = (8+7) Mod 26 (i)
= 15 (p)

7) = (11+7) Mod 26 (l)
= 18 (s)

8) = (18+7) Mod 26 (s)
= 25 (z)

9) = (6+7) Mod 26 (g)
= 13 (n)

10) = (14+7) Mod 26 (o)
= 21 (v)

Caesar cipher Decryption
$D_M(v) = (v-k) \text{ Mod } M$

We shall overcome
px latee hoxkvhfx

1) W = (22-7) Mod 26
= 15 Mod 26
= 41 Mod 26
= 15 (p)

2) = (11-7) Mod 26
= 4 Mod 26
= 30 Mod 26
4 (e)

3) e = (4-7) Mod 26
= -3 Mod 26
= 23 Mod 26
= 49 Mod 26
23 (x)

4) s = (18-7) Mod 26
= 11 Mod 26
= 37 Mod 26
= 11 (l)

5) h = (7-7) Mod 26
= 0 Mod 26
= 26 Mod 26
= 0 (a)

6) a = (0-7) Mod 26
-7 Mod 26
19 Mod 26
35 Mod 26
19 (t)

7) O = (14-7) Mod 26
7 Mod 26
33 Mod 26
7 (H)

8) V = (21-7) Mod 26
14 Mod 26
40 Mod 26
14 (O)

9) K = (17-7) Mod 26
10 Mod 26
36 Mod 26
10 (K)

10) C = (2-7) Mod 26
-5 Mod 26
21 Mod 26
47 Mod 26
21 (V)

11) O = (14-7) Mod 26
7 Mod 26
33 Mod 26
7 (H)

12) M = (12-7) Mod 26
5 Mod 26
31 Mod 26
5 (F)

{≡} congruent

Two int a and b are said to be congruent if
a≡b (Mod M) ⇔ a Mod M = b Mod M

Mathematics of Cryptography

Modular Arithmetic and Congruence

(+ve, -ve) any int = N = qM + R (+ve int)
quotient, remainder

1) -50 Mod 10
-50 = -5 X 10 + R
-50 + 50 = R
R = 0

2) -51 Mod 10
-51 = -6 X 10 + R
-51 + 60 = R
R = 9

3) 60200 Mod 11
60200 %. 11
= 8

4) 2 X 4 Mod 11
8 %. 11
8

5) 73 ≡ 4 (Mod 23)
73 %. 23 = 4 %. 23
4 = 4
Congruent ≡

6) -10 Mod 3
-10 = q X 3 + R
-10 = -4 X 3 + R
R = 2

7) 113 Mod 24
113 %. 24
7

8) -29 Mod 7
-29 = q X 7 + R
-29 = -5 X 7 + R
R = 6

9) 3 ≡ 3 (Mod 17)
3 %. 17 = 3 %. 17
3 = 3 congruent ≡

How to find modulus of -ve number (Mod (2))

Ex - N-Mod m

Method

$N = qM + R$

N or M → int no

R → remainder

q → we have to choose q such that we get more or equal -ve no than n.

Evaluate

1) $(200 - 301) \bmod 11 = (2 * 4) \bmod 11$

$-101 \bmod 11 \quad 8 \bmod 11$

$-101 + 110 = R \quad 8$

$R = 9 \quad 8$

$9 \neq 8$

200 and 11 | 301 and 11 | (2 - 4) and 11 | -2

$-2 = q(11) + R$

$R = 9.$

2) $(200 + 301) \bmod 11 = (2 * 4) \bmod 11$

$501 \bmod 11 = 8 \bmod 11$

$6 \neq 8$

3) $123 * 62 \bmod 12$

$(123 \% 12 * 62 \% 12) \% 12$

$(3 * 2) \% 12$

$6 \% 12$

$\boxed{6}$ Ans

Usage of Modular Arithmetic

Modular arithmetic is very well understood in terms of algorithms for various basic operations. That is one of the reason why we use finite fields (AES) in symmetric key cryptography. Cryptography requires hard problems. Some problems become hard with modular arithmetic.

For eg algorithms are easy to compute are all integers but can become hard to compute when you introduce a modular reduction.

Similarly with finding roots

Mod arithmetic is the central mathematical concept in cryptography. Almost any cipher from the ceaser cipher to the RSA cipher use it.

There are two types of Mod

- The Mod function
- The (Mod) congruence

Modular arithmetic is the branch of arithmetic Mathematics related with the 'Mod' functionality. Basically, Modular arithmetic is related with computation of 'Mod' of expressions

Expressions may have digits and computational symbols of addition, subtraction, multiplication, division or any other. Here we will discuss briefly about all modular arithmetic operations.

Congruent modulo/ congruence cryptography

Congruent number
Integers that leave the same remainder when divided by the modulus n are somehow similar, however not identical. Such members are called 'congruent'. For instance 1 and 13 and 25 and 37 are congruent mod 12 since they all leave the same remainder when divided by 12

To show that two integers are congruent we use the congruence operator (≡)
For eg we write
$(a \bmod n) \equiv (b \bmod n)$
This written as
$a \equiv (b \bmod n)$ or
$b \equiv (a \bmod n)$

Example
- $73 \equiv 4 \pmod{23}$
  $73 \bmod 23 \equiv 4 \bmod 23$
- $2 \equiv 12 \pmod{10}$
  $2 \bmod 10 \equiv 12 \bmod 10$
- Is $6 \equiv 11 \pmod{5}$
  Yes $6 \bmod 5 \equiv 11 \bmod 5$
- Is $7 \equiv 15 \pmod{5}$
  NO $7 \bmod 5 \not\equiv 15 \bmod 5$

Set of Residues
The modulo operation creates a set which is modular arithmetic is referred to as the set of least residues modulo n or Z_n.

Some Z_n sets

$Z_n = \{0, 1, 2, 3, \ldots, (n-1)\}$
$Z_2 = \{0, 1\}$ $Z_6 = \{0, 1, 2, 3, 4, 5\}$
$Z_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

Which of the following is true?

1) $3 \equiv 3 \pmod{17}$ True
2) $3 \equiv -3 \pmod{17}$ False
3) $172 \equiv 177 \pmod{5}$ True
4) $-13 \equiv 13 \pmod{26}$ True

Modular Arithmetic Operation Properties

First Property
$(a+b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$

Second Property
$(a-b) \bmod n = [(a \bmod n) - (b \bmod n)] \bmod n$

Third Property
$(a \times b) \bmod n = [(a \bmod n) \times (b \bmod n)] \bmod n$

→ First Property

Let $A = 14 \quad B = 17 \quad C = 5$

L.H.S $(A+B) \bmod C = (14+17) \bmod 5$
$= 31 \bmod 5$
$= 1$

L.H.S $[(a \bmod c) + (b \bmod c)] \bmod c$
$[(14 \bmod 5) + (17 \bmod 5)] \bmod 5$
$(4+2) \bmod 5$
$6 \bmod 5$
1
$\therefore$ L.H.S = R.H.S

Same goes for Second & Third Property

Q Determine whether 17 is congruent to 5 modulo 6, and whether 24 and 14 are congruent modulo 6

$17 \equiv 5 \pmod 6$ $\quad 17-5 = 12$
$17 \bmod 6 \equiv 5 \bmod 6$ $\quad$ Multiple of 6
$5 \equiv 5$

$24 \equiv 14 \pmod 6$ $\quad 24-14 = 10$
$24 \bmod 6 \equiv 14 \bmod 6$ $\quad$ not a multiple of 6
$0 \neq 2$

Q Evaluate

1) $100 \bmod 26$ 22
2) $126 \bmod 26$ 22
3) $13 \bmod 26$ 13
4) $-5 \bmod 26$ $-5+26 = 21$
5) $12 \bmod 26$ 12

Sunil
DATE
PAGE
"Rough 'n' Fair"

Q Solve

1) $5+10 \mod 26$ — 15
2) $13-16 \mod 26$ — 7
3) $32+46 \mod 26$ — 0

Q Add 7 to 14 in 215

$7+14 \mod 15$

$21 \mod 15$

6

Q Subtract 11 from 7 in 213

$7-11 \mod 13$

$(7 \mod 13 - 11 \mod 13) \mod 13$

$(7-11) \mod 13$

$-4 \mod 13$

$-14+13 = R$

$R = 9$

Q Multiply 11 by 7 in 220

$11 \times 7 \mod 20$

$77 \mod 20$

17

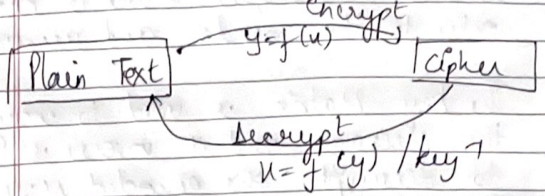
Q $7^2 \pmod{13}$

$49 \mod 13$

10

Sunil
DATE
PAGE
"Rough 'n' Fair"

Matrices in Cryptography



Q $-13 \simeq 13 \mod 26$ check whether it is valid or invalid

$-13 \equiv 13 \mod 26$

$-13 = -1 \times 26 + R \equiv 13$

$13 \equiv 13$

$-13 \simeq 13 \mod 26$ — false — they are congruent

Q One of the application (important) of inverse of a square matrix is in cryptography

Cryptography is an art of communication b/w two people by keeping the info not known to others. It is based upon two factors i.e

Encryption

Decryption

Encryption & Decryption requires a secret technique which is known only to the sender and receiver.

Note: The key matrix is used to encrypt the message and it inverse is used to decrypt the encoded message. It is important that key matrix is keep secret between the message sender and receiver.
If the key matrix or it inverse is discovered that all the user all hackers can easily decode the message.

Eg $A = \begin{bmatrix} 1 & -1 & 1 \\ 2 & -1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$

Message = "Welcome"
(WEL) (COM) (E00)

Uncoded matrix	Encoding matrix	Coded row matrix
[23,5,12]	$\begin{bmatrix} 1 & -1 & 1 \\ 2 & -1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$	[45, -28, 23]
[3,15,13]	$\begin{bmatrix} 1 & -1 & 1 \\ 2 & -1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$	[46, -18, 3]
[5,0,0]	$\begin{bmatrix} 1 & -1 & 1 \\ 2 & -1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$	[5, -5, 5]

decoding matrix = $A^{-1} = \frac{1}{|A|} \text{adj } A$ $\quad \begin{bmatrix} 0 & 0 & 1 \\ 0 & -1 & 2 \\ 1 & -1 & 1 \end{bmatrix}$

$|A| = 1(0-0) - (-1)(0-0) + 1(0+1)$
$= 0 - 0 + 1$
$= 1$

Q. Encrypt the message "COVID" using the encryption matrix

$\begin{bmatrix} 1 & -1 & 1 \\ 2 & -1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$

COV IDO

[3,15,22]	$\begin{bmatrix} 1 & -1 & 1 \\ 2 & -1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$	[55, -18, 3]
[9,4,0]	$\begin{bmatrix} 1 & -1 & 1 \\ 2 & -1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$	[17, -13, 9]

decoding matrix $\frac{1}{|A|} \text{adj } A$ $\quad \begin{bmatrix} 0 & 0 & 1 \\ 0 & -1 & 2 \\ 1 & -1 & 1 \end{bmatrix}$