COS30015 IT Security

Week 7

Presented by YICUN TIAN (YI)

18 Sep 2024

Acknowledgement of Country

We respectfully acknowledge the Wurundjeri People of the Kulin Nation, who are the Traditional Owners of the land on which Swinburne's Australian campuses are located in Melbourne's east and outer-east, and pay our respect to their Elders past, present and emerging.

We are honoured to recognise our connection to Wurundjeri Country, history, culture, and spirituality through these locations, and strive to ensure that we operate in a manner that respects and honours the Elders and Ancestors of these lands.

We also respectfully acknowledge Swinburne's Aboriginal and Torres Strait Islander staff, students, alumni, partners and visitors.

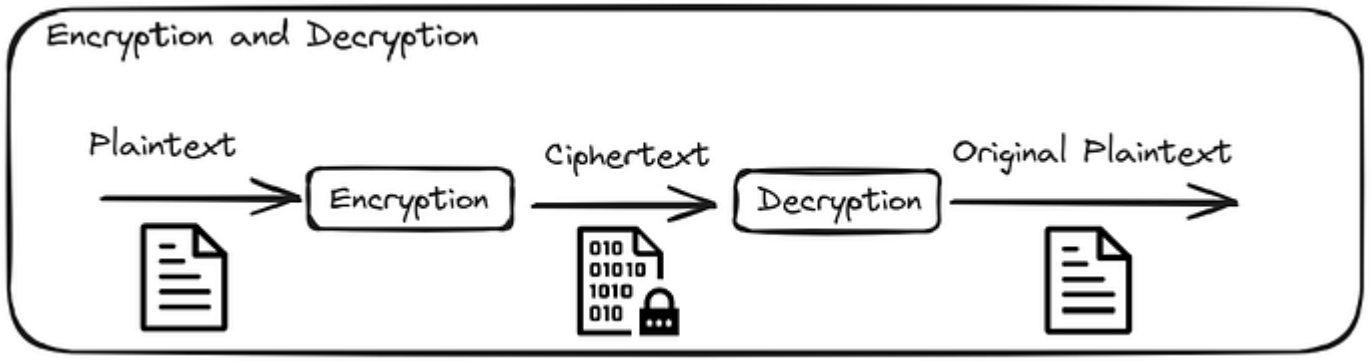
We also acknowledge and respect the Traditional Owners of lands across Australia, their Elders, Ancestors, cultures, and heritage, and recognise the continuing sovereignties of all Aboriginal and Torres Strait Islander Nations.

Cryptography

Terminology

Suppose a sender wants to send a message to a receiver. She wants to make sure an eavesdropper cannot read the message.

- Message or Plaintext: it can be a stream of bits, a text file, a bitmap, audio, video, etc. and can be intended for either transmission or storage.
- Encryption: process of hiding a message.
- Ciphertext: encrypted message.
- Decryption: process of turning ciphertext back into plaintext



- Unconditional Security
- one-time pad
- Brute-Force Attack
- Computational Security

https://bzambelli.medium.com/cryptography-fundamentals-bf4a525cc7b1

Two general types of key-based algorithms

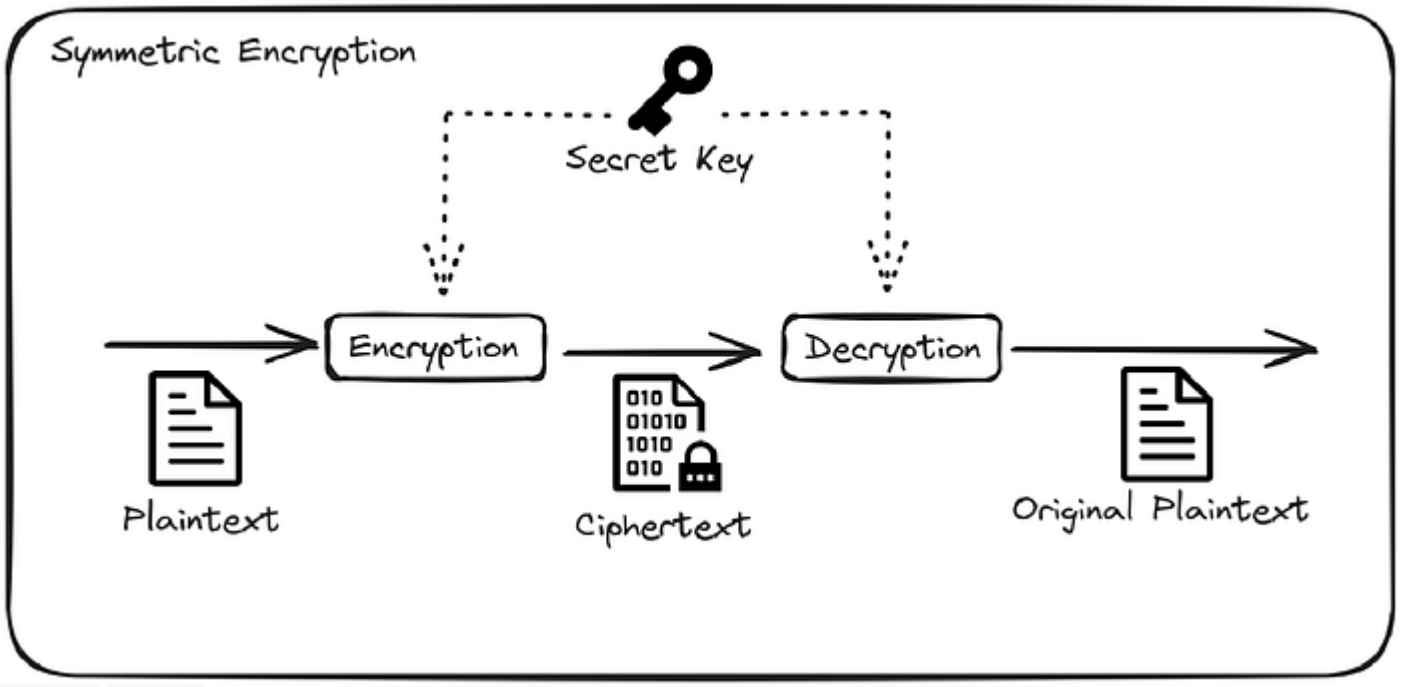
- Symmetric Encryption
  - Caesar Cipher
  - Vigenère Cipher
  - DES (Data Encryption Standard)
  - AES (Advanced Encryption Standard)
  - DES vs AES

- Public-Key (also called Asymmetric Encryption).
  - RSA (Rivest–Shamir–Adleman)

Type - Symmetric Cryptography

Symmetric Cryptography:

- **Single Key**: Symmetric cryptography uses a single secret key for both encryption and decryption. This key must be kept confidential and known only to the parties involved.
- **Efficiency**: Symmetric encryption algorithms are generally **faster** and more computationally efficient than asymmetric algorithms. They are suitable for encrypting **large amounts of data**.
- **Key Management**: Key distribution and management can be challenging, especially in large-scale systems, as each pair of communicating parties needs to share a common secret key securely.



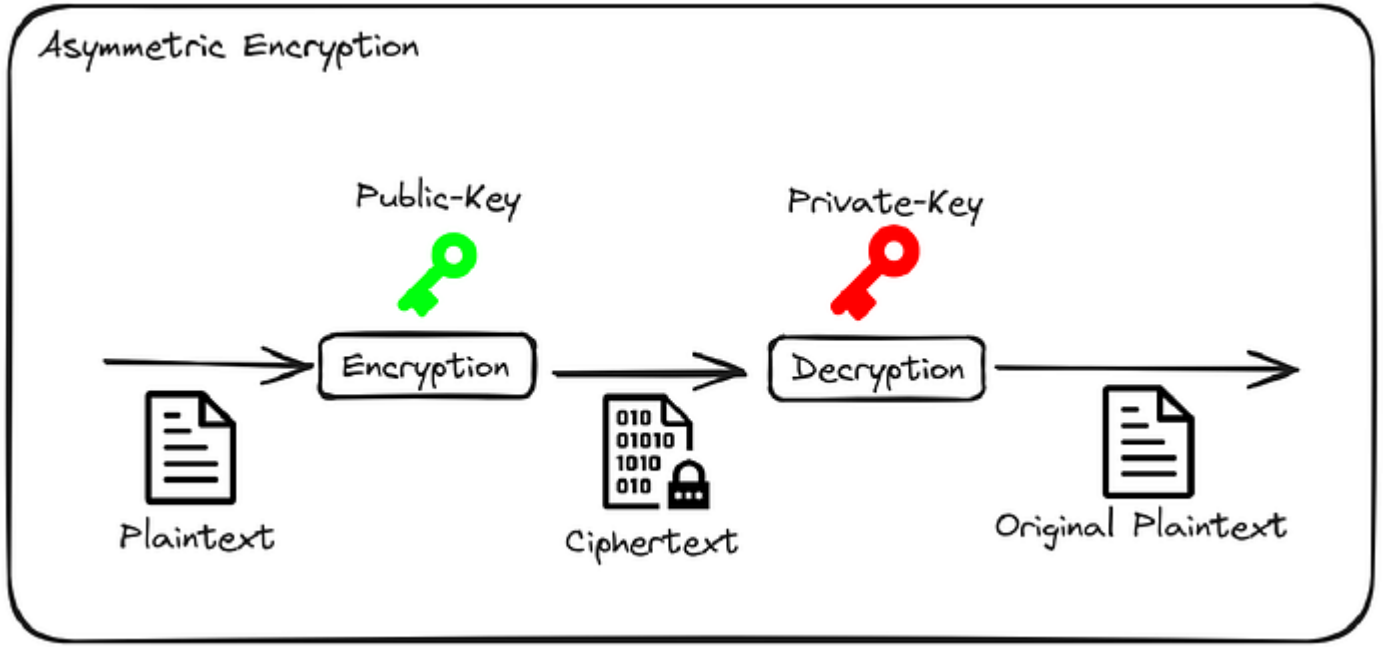
https://bzambelli.medium.com/c...

SWINBURNE UNIVERSITY OF TECHNOLOGY

Type - Asymmetric Cryptography

Asymmetric Cryptography (Public-Key Cryptography):

- **Key Pair**: Asymmetric cryptography uses a pair of keys: a public key and a private key. The public key is widely distributed and used for encryption, while the private key is kept secret and used for decryption.
- **Security and Key Exchange**: Asymmetric cryptography provides a solution to the key distribution problem in symmetric cryptography. Public keys can be freely shared, allowing anyone to encrypt data for the owner of the corresponding private key.
- **Digital Signatures**: Asymmetric cryptography is often used for digital signatures, where the private key is used to sign data, and the public key is used to verify the signature.

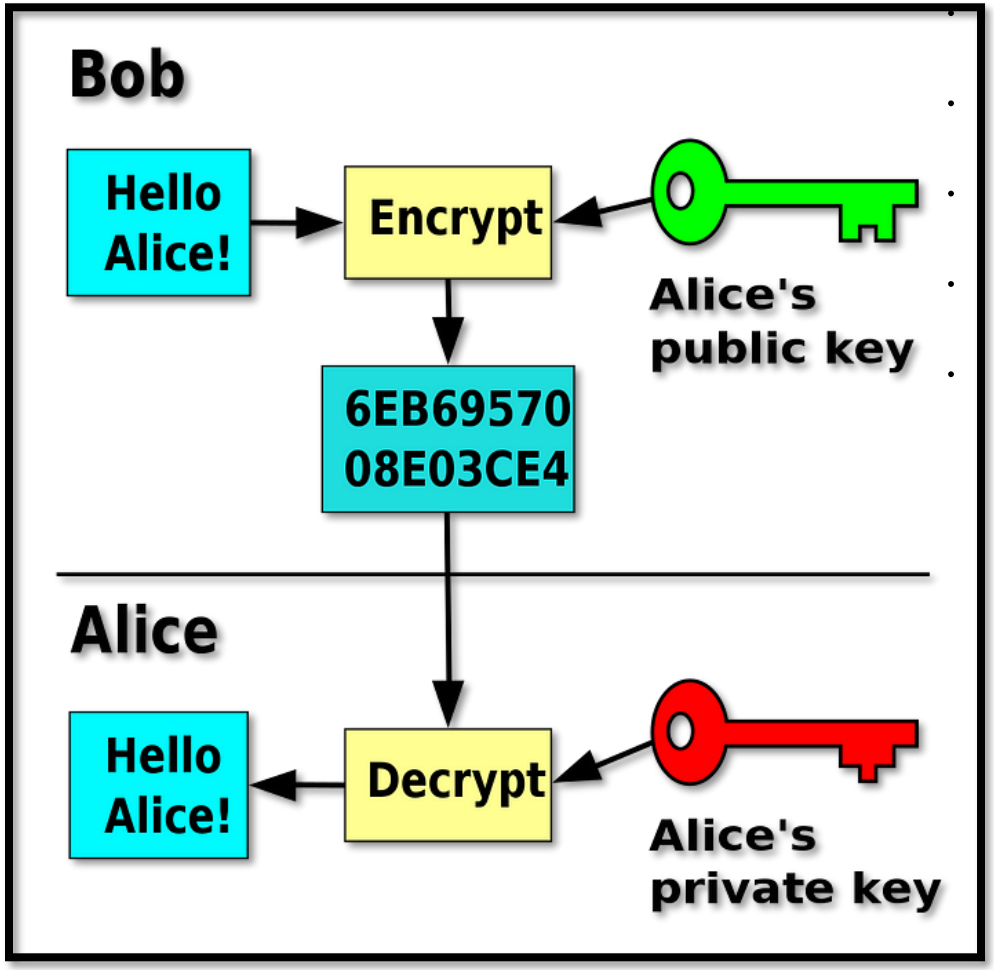


Asymmetric Cryptography - Example

Public-Key Real World Example

Imagine you want to send a secret message to your friend, but you're worried about someone intercepting it. Public-key encryption can help.

- You and your friend each have a pair of keys: a public key and a private key.
- Your public key is like a padlock that everyone can see, but only your private key can unlock it.
- You lock your message with your friend's public key and send it.
- Only your friend, who has the corresponding private key, can unlock and read the message



https://bzambelli.medium.com/cryptography-fundamentals-bf4a525cc7b1

Substitution Cipher (Caesar Cipher):

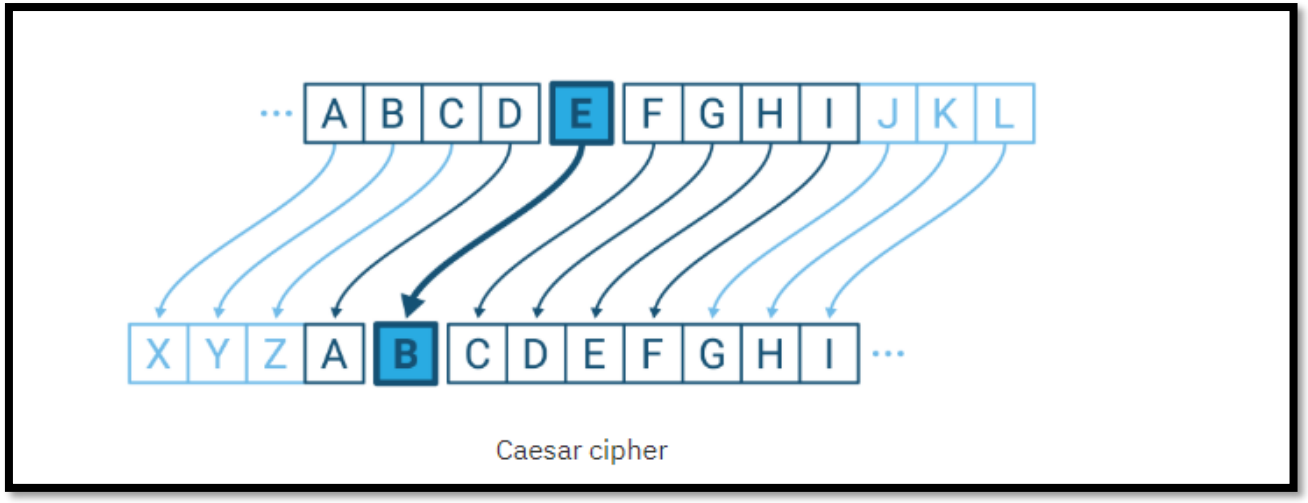
In a Caesar cipher, each letter in the plaintext is shifted **a fixed number of positions down or up** the alphabet.

Plaintext: "HELLO"

Shift: 3

Ciphertext: "EBIIL“

Here, each letter in the plaintext has been shifted three positions up the alphabet to produce the ciphertext.



Caesar cipher

https://community.ibm.com/community/user/ibmz-and-linuxone/blogs/subhasish-sarkar1/2020/07/04/caesar-cipher

Security – Caesar Cipher

- **Not considered secure** for modern encryption purposes
- Reason:
    1) With only **26 possible shift values** in the English alphabet (assuming a standard Caesar Cipher), an attacker can easily try all possible shifts to decrypt the message using a **brute-force attack**
    2) **Does not obscure letter frequencies**, making it vulnerable to frequency analysis.

Polyalphabetic Cipher (Vigenère Cipher)

Key Components:

- **Plaintext - original message**
- **Keyword - a secret word or phrase**

Encryption Process:

- **Choose a Keyword**: Select a secret keyword that is as long as or longer than the plaintext message.
- **Repeat the Keyword**: If the keyword is **shorter** than the plaintext, repeat it to match the length of the plaintext.
- **Encrypt the Message -** For each letter in the plaintext:
  - Find the corresponding letter in the keyword.
  - Use the Caesar Cipher principle to shift the letter in the plaintext by the value of the corresponding keyword letter.
  - Record the resulting letter in the ciphertext.

Polyalphabetic Cipher (Vigenère Cipher)

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Vigenère cipher key

D	O	G

Plaintext

L	O	A	D

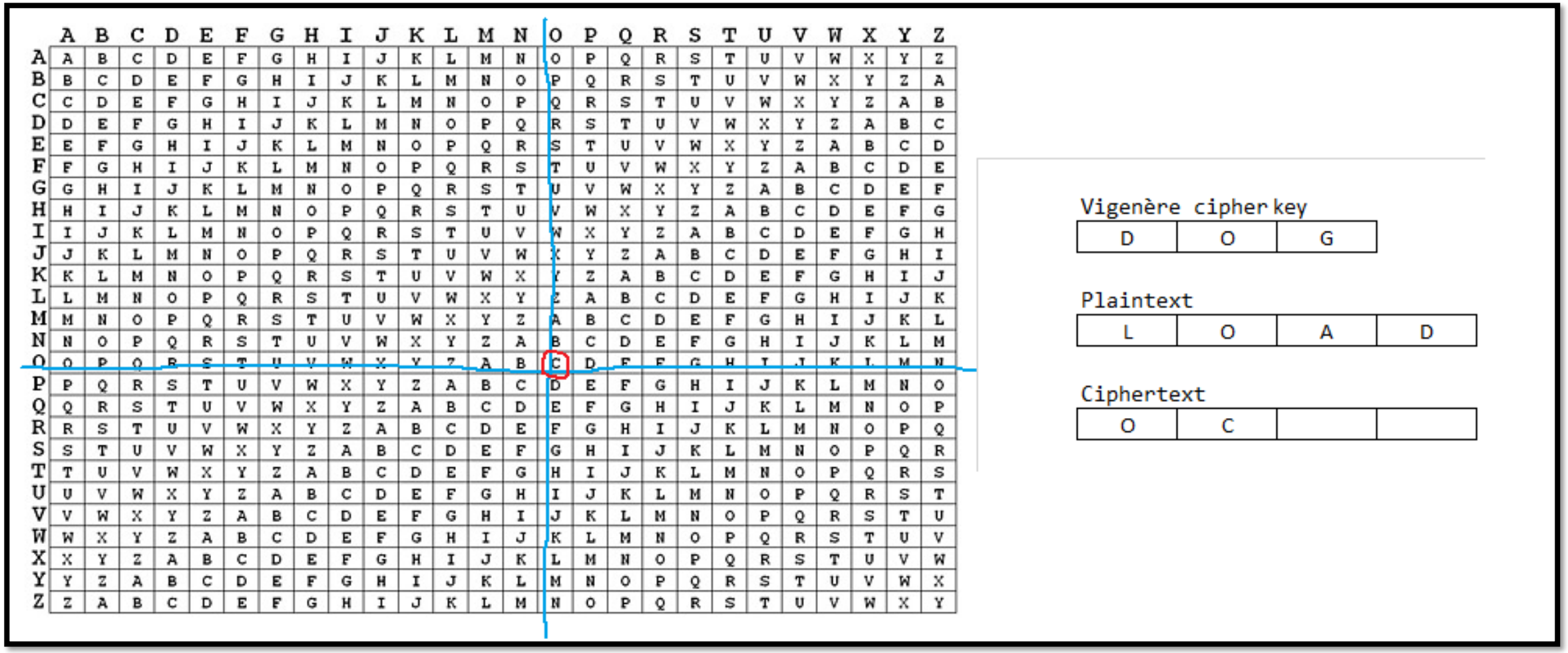
Ciphertext

O			

https://community.ibm.com/community/user/ibmz-and-linuxone/blogs/subhasish-sarkar1/2020/07/17/how-much-do-you-know-about-the-vigenere-cipher

SWINBURNE UNIVERSITY OF TECHNOLOGY

Polyalphabetic Cipher (Vigenère Cipher)



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Vigenère cipher key

D	O	G

Plaintext

L	O	A	D

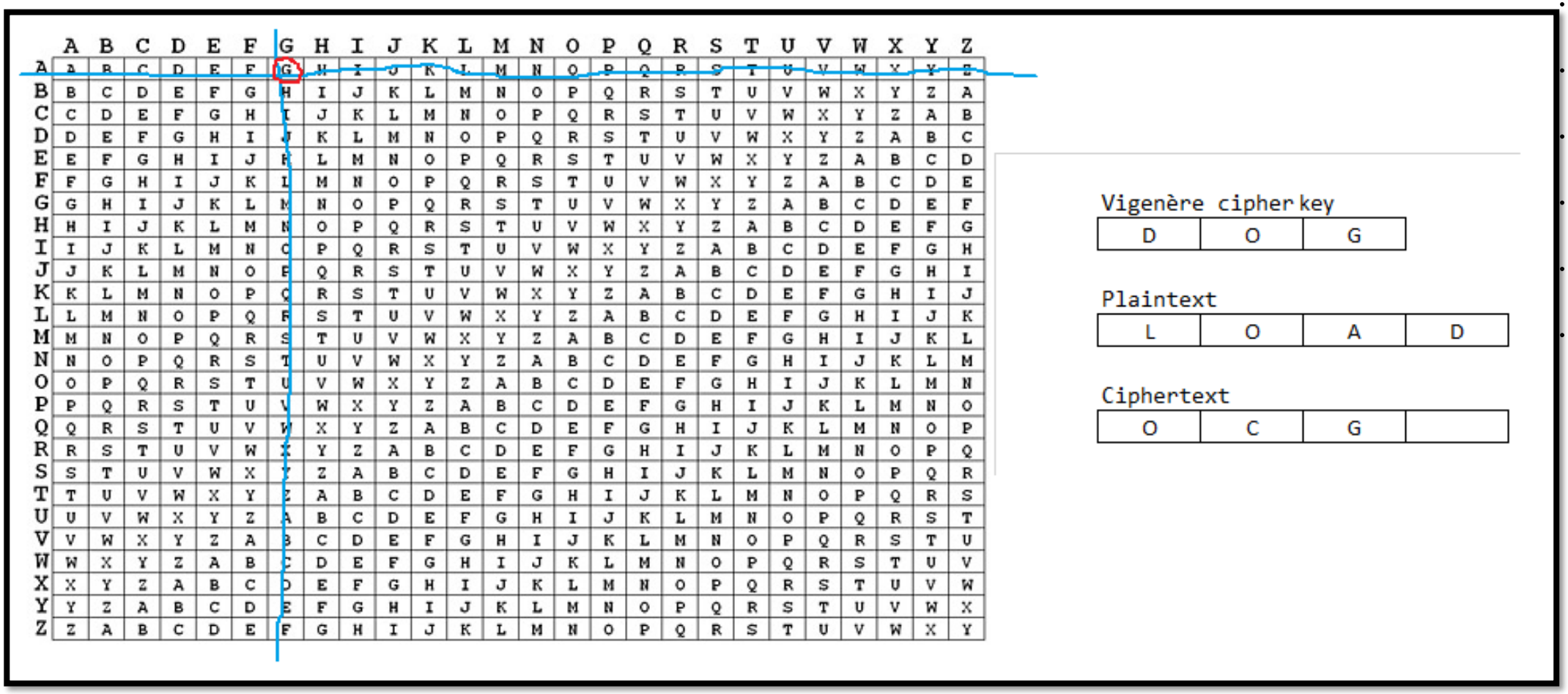
Ciphertext

O	C		

https://community.ibm.com/community/user/ibmz-and-linuxone/blogs/subhasish-sarkar1/2020/07/17/how-much-do-you-know-about-the-vigenere-cipher

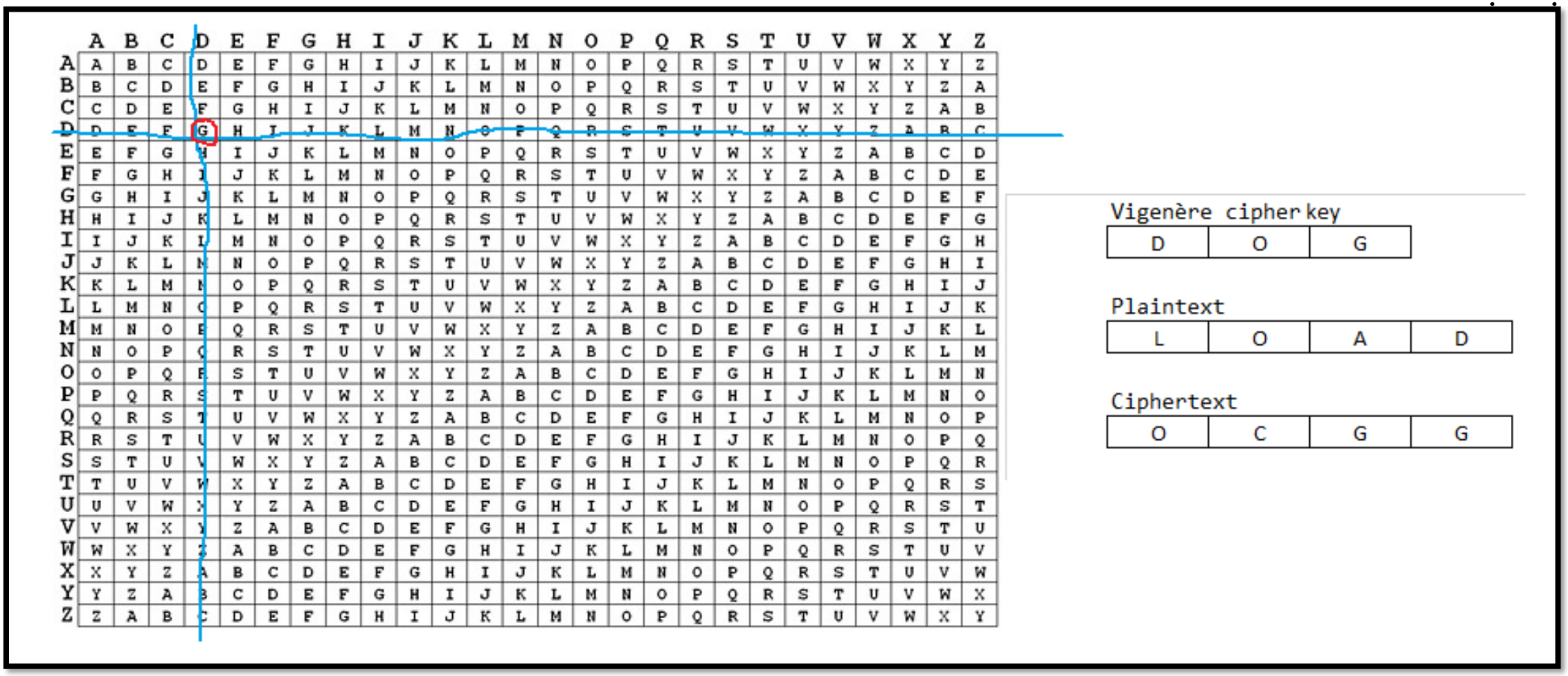
SWINBURNE UNIVERSITY OF TECHNOLOGY

Polyalphabetic Cipher (Vigenère Cipher)



https://community.ibm.com/community/user/ibmz-and-linuxone/blogs/subhasish-sarkar1/2020/07/17/how-much-do-you-know-about-the-vigenere-cipher

Polyalphabetic Cipher (Vigenère Cipher)



https://community.ibm.com/community/user/ibmz-and-linuxone/blogs/subhasish-sarkar1/2020/07/17/how-much-do-you-know-about-the-vigenere-cipher

DES (Data Encryption Standard)

How It Works:

1. Input and Initial Permutation

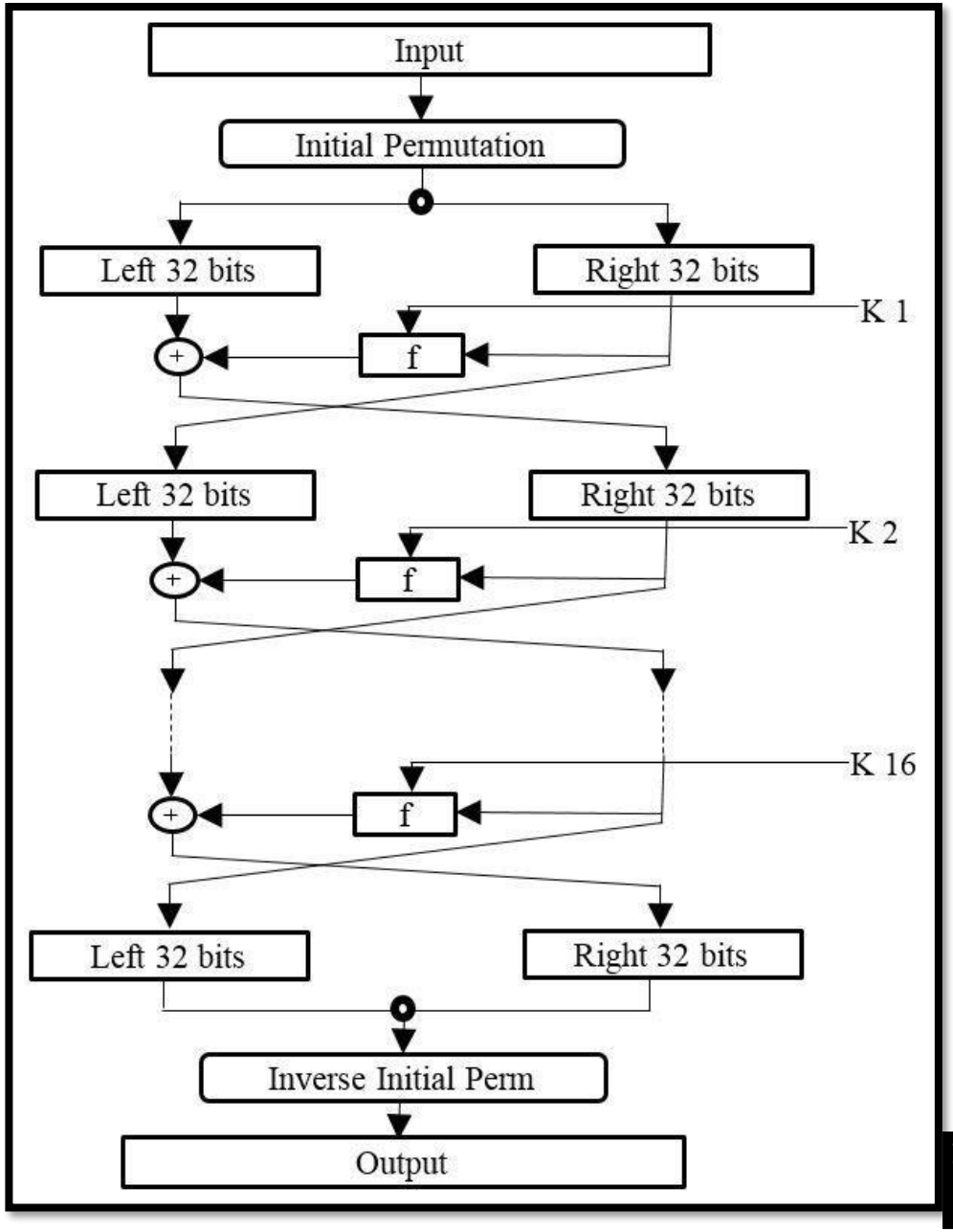
- Input block
- Initial Permutation: rearranging the bits to increase confusion. The data is split into two halves: Left 32 bits and Right 32 bits

2.Key Generation: DES uses a 56-bit key, but only **48 bits are used for encryption**, with the remaining bits used for parity and control.

3.The 16 Rounds of Processing

- Expansion
- Key Mixing
- Substitution via S-boxes
- Permutation
- Combination

4.Final Permutation



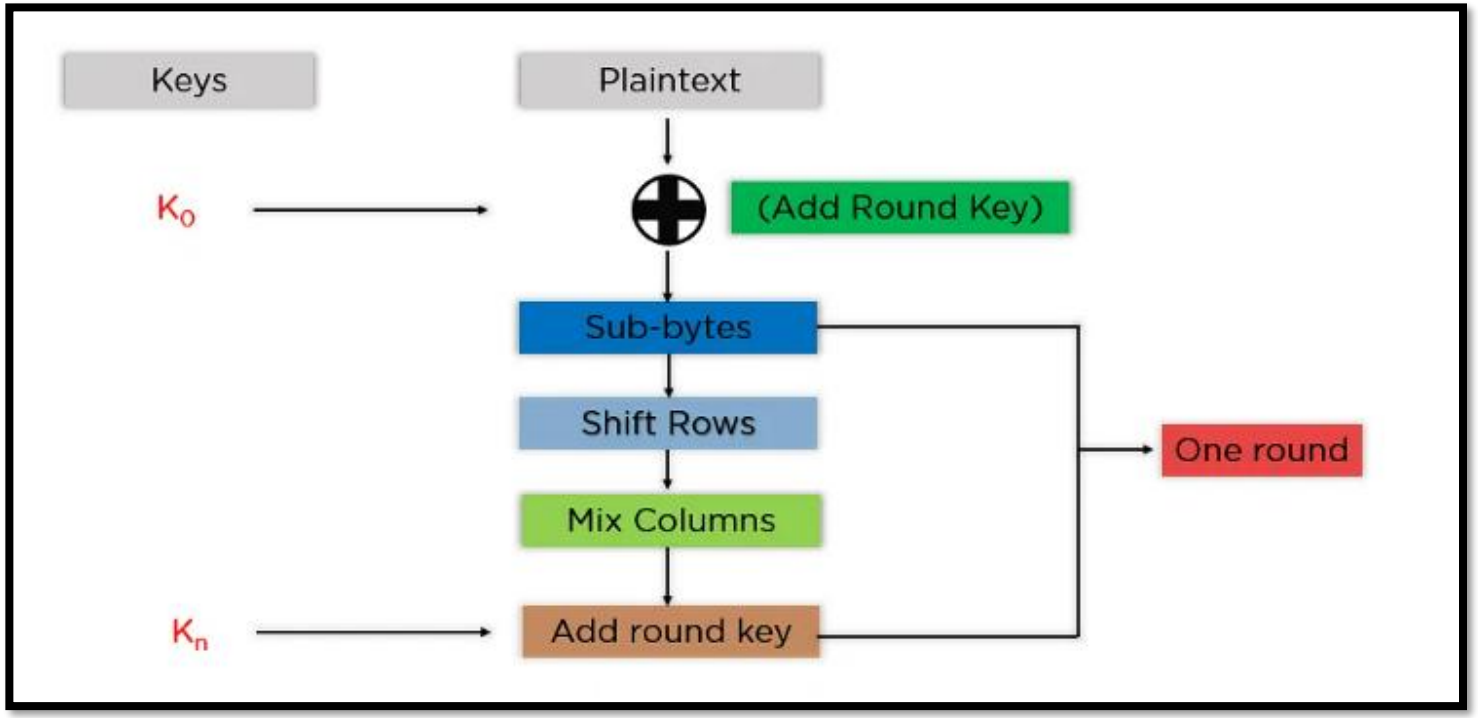
https://www.researchgate.net/figure/Data-Encryption-Standard-DES-Algorithm_fig4_321587376

SWINBURNE UNIVERSITY OF TECHNOLOGY

AES (Advanced Encryption Standard)

Encryption Process:

The AES encryption process involves several steps, including SubBytes (substitution), ShiftRows, MixColumns, and AddRoundKey operations in each round. The encryption process is reversible, meaning that the decryption process reverses each step.

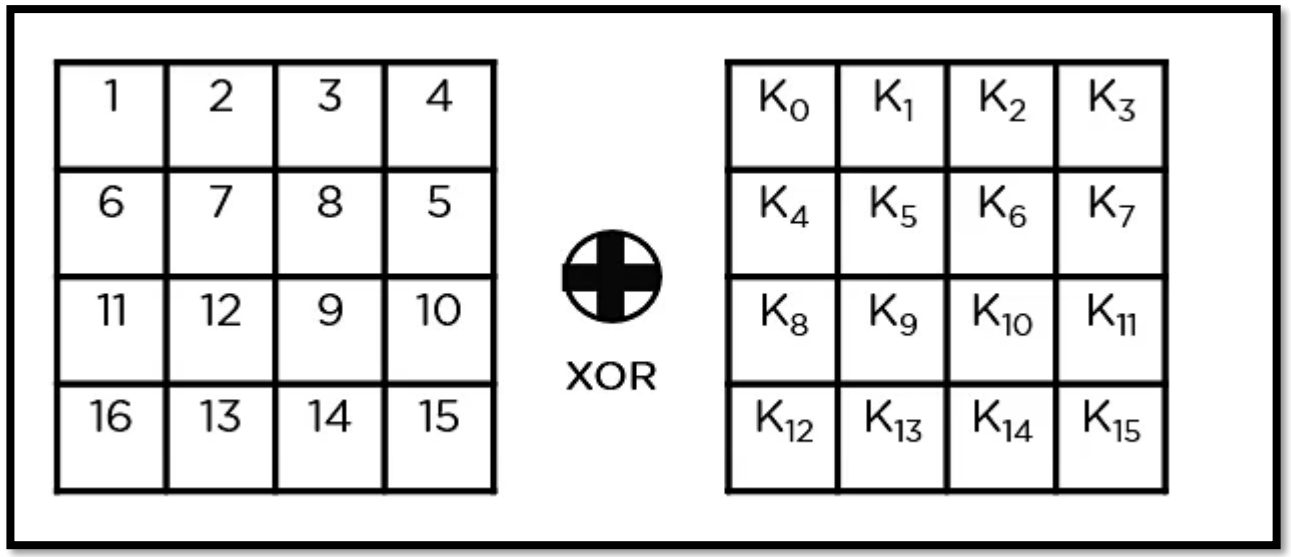


https://www.simplilearn.com/tutorials/cryptography-tutorial/aes-encryption

AES (Advanced Encryption Standard)

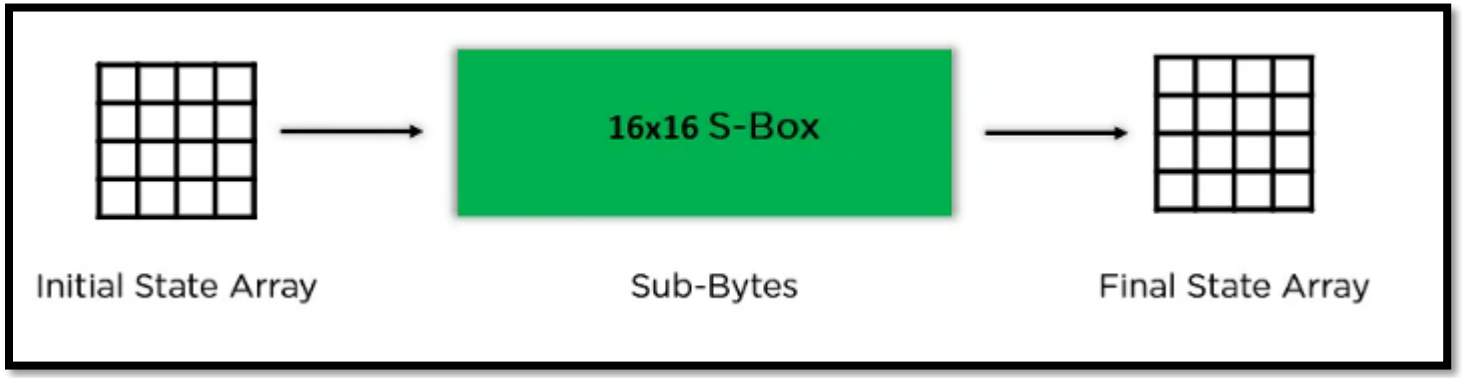
Add Round Key

- pass the block data stored in the state array through an **XOR function** with the first key generated (K0).



Sub-Bytes

- Each byte in the block of plaintext is replaced with a corresponding byte from the AES S-box (Substitution box).
- S-box is a predefined lookup table that performs a byte-by-byte substitution.



https://www.simplilearn.com/tutorials/cryptography-tutorial/aes-encryption

SWINBURNE UNIVERSITY OF TECHNOLOGY

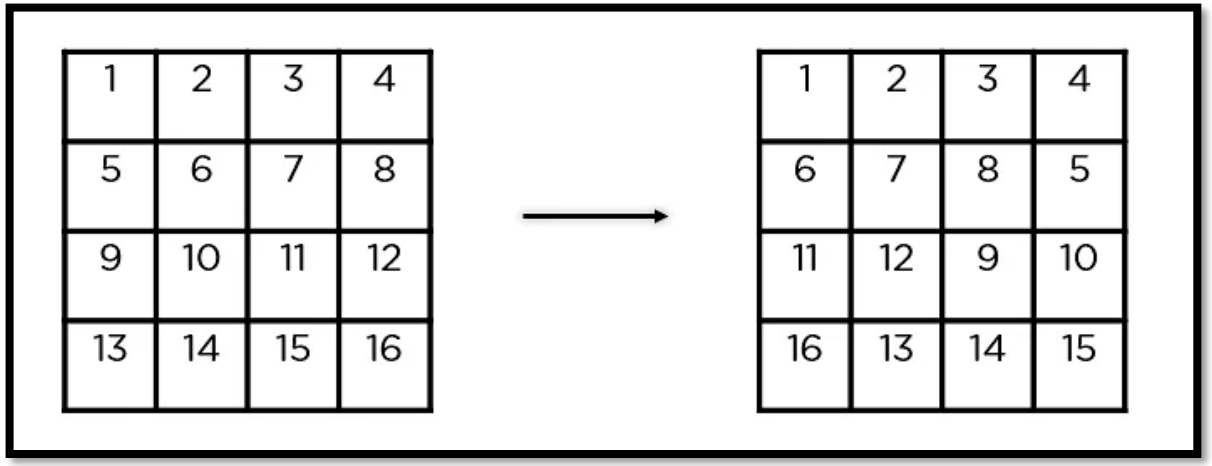
AES (Advanced Encryption Standard)

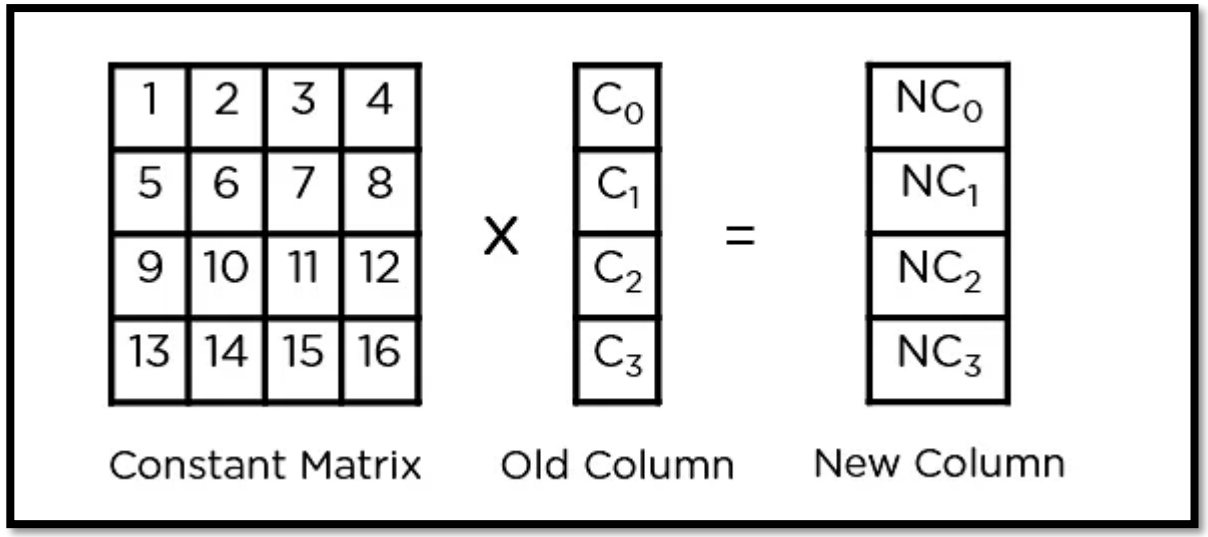
Shift Rows

- The bytes within each row of the block are shifted to the left.

- 1st row – same

- 2nd row is shifted 1 byte





MixColumns

- each column is treated as a **polynomial**, and **matrix multiplication** is performed on each column separately

- provides additional security

https://www.simplilearn.com/tutorials/cryptography-tutorial/aes-encryption

AES - EXAMPLE

Plaintext – Two One Nine Two

T	w	o		O	n	e		N	i	n	e		T	w	o
54	77	6F	20	4F	6E	65	20	43	69	6E	25	20	54	77	6F

Plaintext in Hex Format

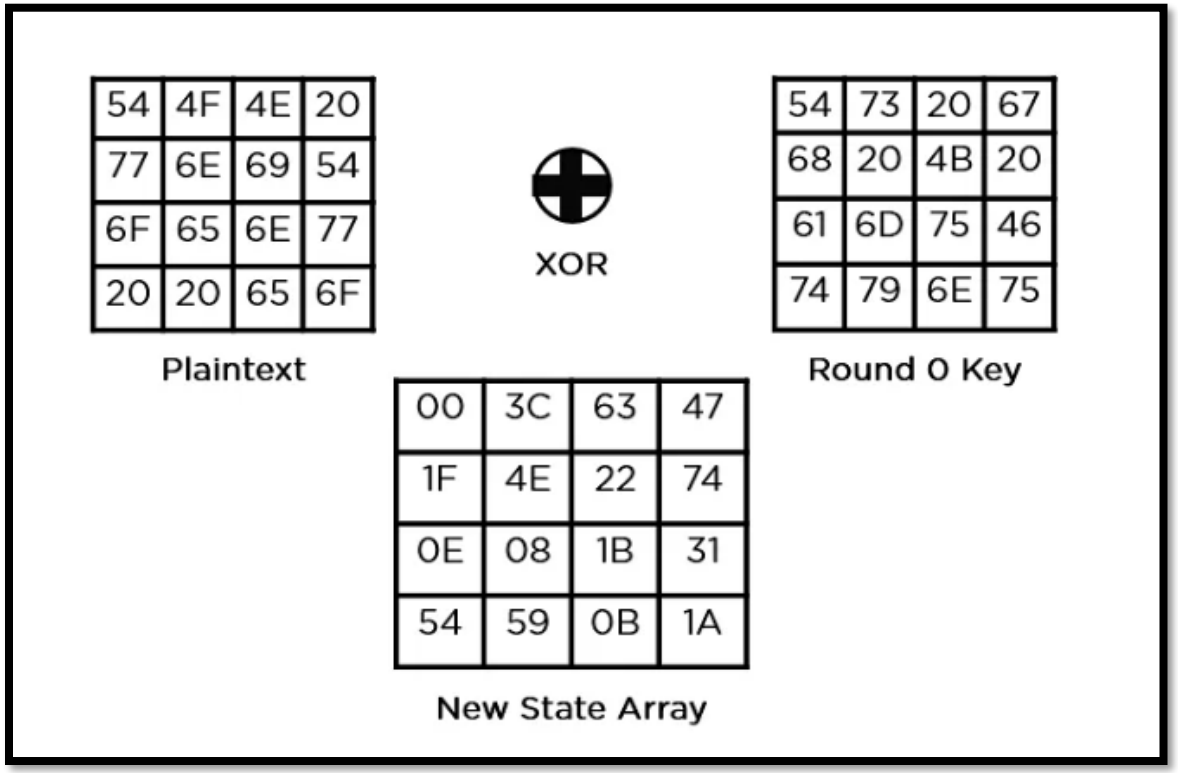
54 77 6F 20 4F 6E 65 20 43 69 6E 25 20 54 77 6F

Encryption Key – Thats my Kung Fu

T	h	a	t	s		m	y		K	u	n	g		F	u
54	68	61	74	73	20	6D	79	20	4B	75	6E	67	20	46	75

Encryption Key in Hex Format

54 68 61 74 73 20 6D 79 20 4B 75 6E 67 20 46 75



https://www.simplilearn.com/tutorials/cryptography-tutorial/aes-encryption

SWINBURNE UNIVERSITY OF TECHNOLOGY

AES - EXAMPLE

63	EB	9F	A0
C0	2F	93	92
AB	30	AF	C7
20	CB	2B	A2

New State Array

Shift Rows:

63	EB	9F	A0
C0	2F	93	92
AB	30	AF	C7
20	CB	2B	A2

Old State Array

→

63	EB	9F	A0
2F	93	92	C0
AF	C7	AB	30
A2	20	CB	2B

New State Array

Mix Columns:

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

Constant Matrix

X

63	EB	9F	A0
2F	93	92	C0
AF	C7	AB	30
A2	20	CB	2B

Old State Array

→

BA	84	E8	1B
75	A4	8D	40
F4	8D	06	7D
7A	32	0E	5D

New State Array

Final State Array after Round 10

29	57	40	1A
C3	14	22	02
50	20	99	D7
5F	F6	B3	3A

AES Final Output

29 C3 50 5F 57 14 20 F6 40 22 99 B3 1A 02 D7 3A

↓

Ciphertext

DES vs AES

Advantages

- It can be implemented **on both hardware and software.**
- It provides **high security** to the users.
- It provides one of the best open-source solutions for encryption.
- It is a very robust algorithm.

DES Algorithm	AES Algorithm
Key Length - 56 bits	Key Length - 128, 192, 256 bits
Block Size - 64 bits	Block size - 128 bits
Fixed no. of rounds	No. of rounds dependent on key length
Slower and less secure	Faster and more secure

https://www.simplilearn.com/tutorials/cryptography-tutorial/aes-encryption

Security of Algorithms

- Cryptographic algorithms offer **different security levels based on difficulty to break**.
- Data is safe if the **cost** to break the encryption **exceeds** the value of the encrypted data.
- Data is likely safe if the **time** required to break the encryption **exceeds** the time the data needs to remain confidential.
- **Key reuse** occurs when the same key encrypts different pieces of data.
- **Strong algorithms** should withstand attacks even if encrypted data is intercepted.
- Large amounts of data encrypted with the **same key increase the risk of attack.**
- Effective **key management**, such as periodically changing keys, mitigates risks.
- Limiting data encrypted with a single key reduces the impact of key compromise.

https://bzambelli.medium.com/cryptography-fundamentals-bf4a525cc7b1

Cryptographic Principles

Principles

- Confidential
- Integrity
- Authentication
- Non-repudiation

Challenges of Cryptography

- Key management: Proper handling of keys is essential for secure communication.
- Quantum computing: Future quantum computers may threaten current cryptographic algorithms.
- Human error: Security can be compromised by human mistakes, weakening cryptography.

https://www.geeksforgeeks.org/cryptography-introduction/

Digital Signature

Digital Signature

- **Data integrity**: stays unchanged during transmission or storage
- **Checksum**

- A digital signature is an encrypted stamp of authentication for digital information like messages.
- It confirms the message's **integrity** and proves the sender's **identity**.
- **Any modification** to signed data makes the signature **invalid**.
- Ensure **end-to-end** message integrity and verify the origin.
- Sign the **entire** message or **parts**
- The recipient decrypts the signature using the sender’s public key to verify the message.
- **Only** the **private key** holder can create a signature, but **anyone** with the **public key** can verify it.
- Digital signatures use cryptography and are equivalent to a personal signature.

https://www.ibm.com/docs/en/b2badv-communication/1.0.0?topic=overview-digital-signature

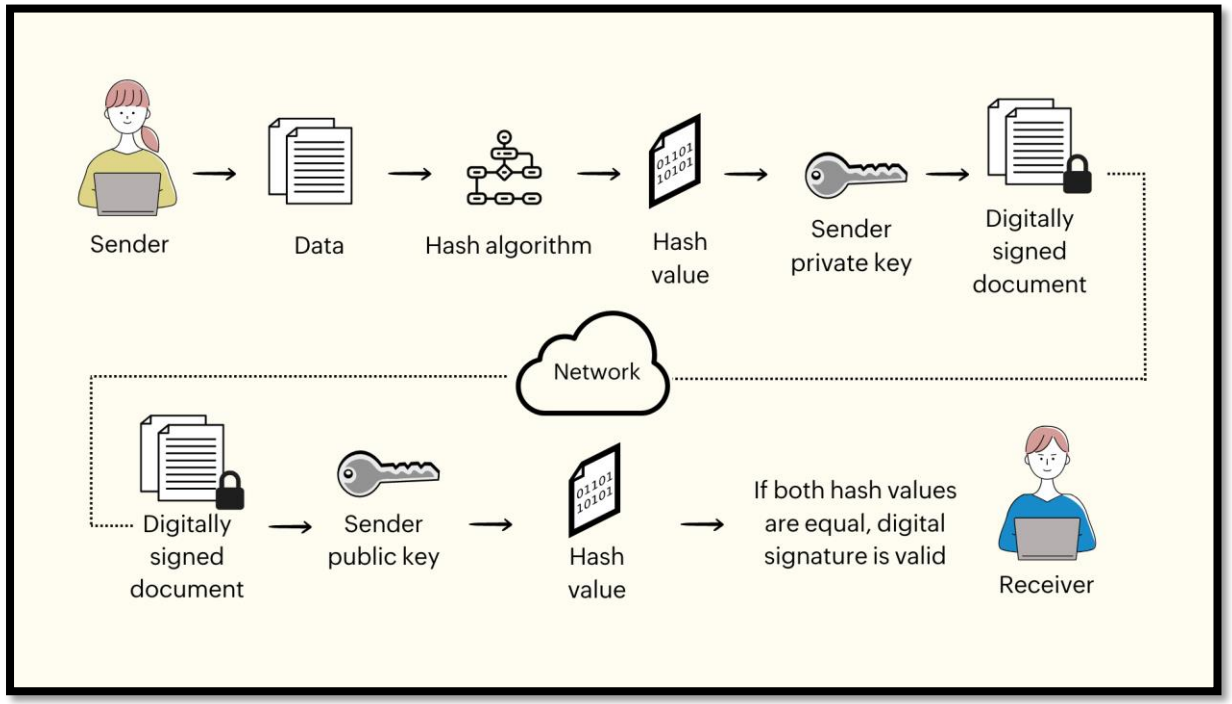
One-way algorithms

- also known as a hash function
- an algorithm that compresses data of any length into a fixed-length value
- even a small change in the data will result in a completely different hash value
- impossible to reverse-engineer the original data from the hash value
- a crucial part of the digital signature process
    - Hash Function (One-way algorithm)
    - Signing Process
    - Verification Process
- common applications
    - Data Integrity Check
    - Password Storage
    - Message Digest
    - Hash Tables

https://www.simplilearn.com/tutorials/cryptography-tutorial/aes-encryption

How does a Digital Signature Work?

1) Signer generates data
2) Hash Algorithm
3) Encrypt the hash value
4) Create a digitally signed document
5) Receiver verifies the signature
6) Validate the hash value



Question:

If the public key and hash algorithm are public, doesn't that mean anyone can intercept and read the original message? Isn't this a flaw?

https://www.simplilearn.com/tutorials/cryptography-tutorial/aes-encryption

Benefits of Digital Signatures

A digital signature is used to assure:

- Authenticity
- Integrity
- Nonrepudiation

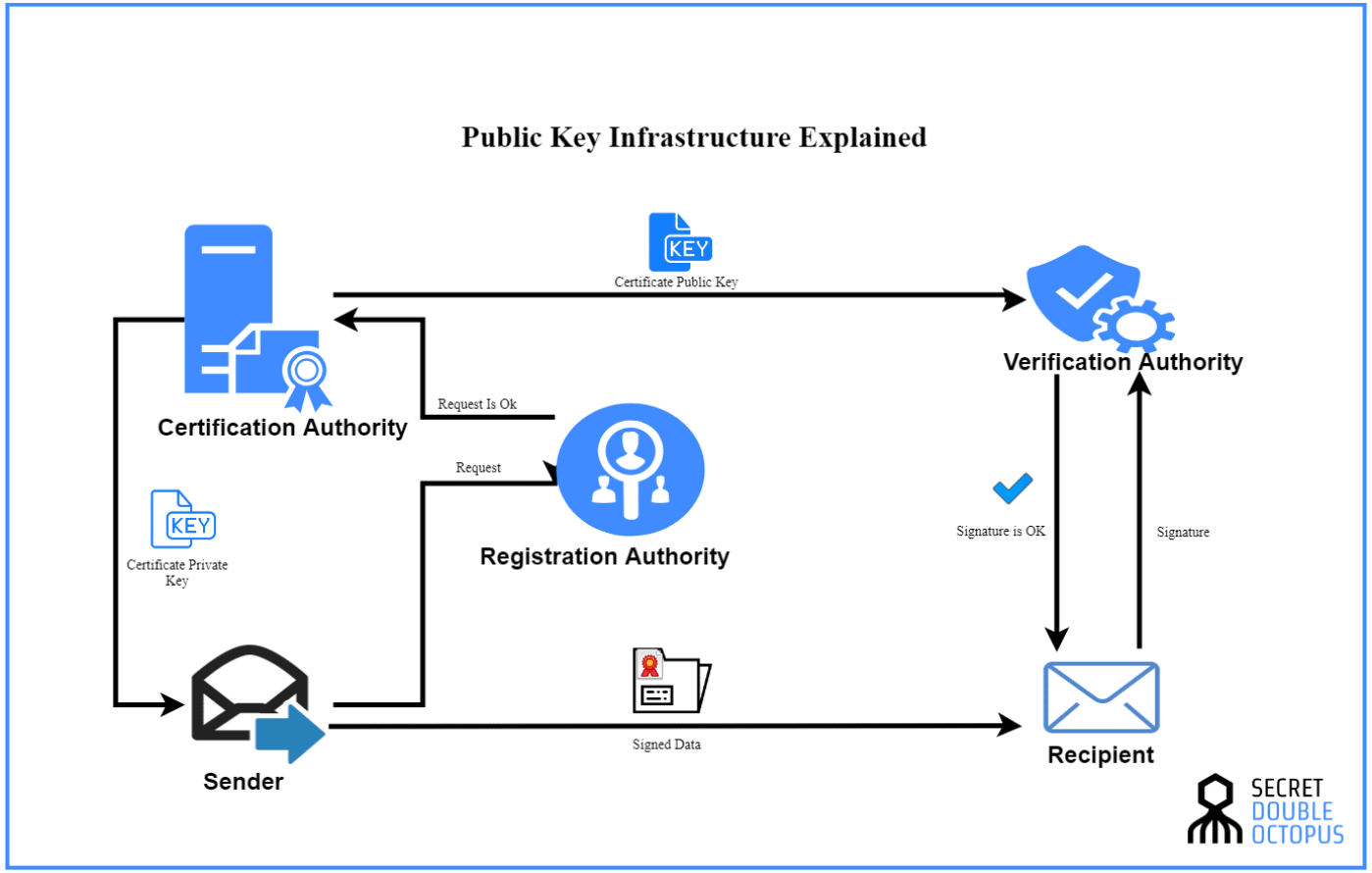
https://www.simplilearn.com/tutorials/cryptography-tutorial/aes-encryption

PGP/GPG (web of trust)

PKI – Public Key Infrastructure

- ✓ RA - Registration Authority
- ✓ CA - Certification Authority
- ✓ VA - Verification Authority

1) Sender Initiates Communication
2) Sender Requests Certification
3) RA Confirms and Forwards to CA
4) Certification Issued
5) Signed Data Sent to Recipient
6) Verification by the VA
7) Recipient Verifies the Signature
8) Message Integrity Confirmed



https://www.simplilearn.com/tutorials/cryptography-tutorial/aes-encryption

SWINBURNE UNIVERSITY OF TECHNOLOGY

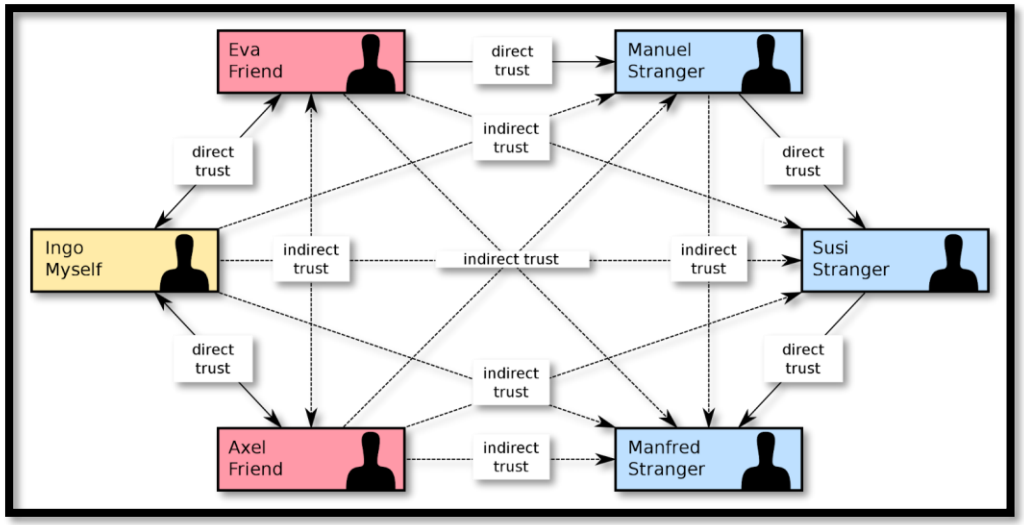
Centralized Certificate Authorities (CAs)

- ✓ A Certificate Authority (CA) is a trusted third party that issues and manages digital certificates.
- ✓ CAs verify identities and sign public keys using their private key, generating digital certificates that prove ownership of a public key.
- ✓ CAs form the core of a centralized trust model, where users and systems trust the CA to validate certificate holders.
- ✓ Digital certificates include the public key, identity information, and expiration date, signed by the CA's private key.
- ✓ The authenticity of a certificate can be verified using the CA's public key.
- ✓ Disadvantages
  - Single Point of Failure
  - Trust Issues:
  - Certificate Costs

Web of Trust

- ✓ The Emergence of Web of Trust:
- ✓ Unlike relying on a single centralized authority, the Web of Trust builds a more flexible trust relationship through mutual signatures and trust between users.
- ✓ Decentralized Trust Model
- ✓ Trust Chains:
  - ✓ Users establish a chain of trust through digital signatures.
  - ✓ For example, if A trusts B and B trusts C, then A may choose to trust C, forming a web of trust.

- ✓ Applications of Web of Trust:
  - ✓ PGP (Pretty Good Privacy)
  - ✓ GPG (GNU Privacy Guard)



https://www.techslang.com/what-is-web-of-trust/

SWINBURNE UNIVERSITY OF TECHNOLOGY

Conclusion

Symmetric Cryptography

- Caesar Cipher
- Vigenère Cipher
- DES (Data Encryption Standard)
- AES (Advanced Encryption Standard)
- DES vs AES

Asymmetric Cryptography (Public-Key Cryptography)

- RSA (Rivest–Shamir–Adleman)

Principles & Challenges

Digital Signature

PGP/GPG (web of trust)

Thanks for Watching