CYBER SECURITY

- RAVIPATI SRINIVASA KALYAN

L23CS216

Contents:

- INTRODUCTION TO CYBER SECURITY
- WHAT IS A THREAT ?
- TYPES OF CYBER ATTACKS
- INFORMATION CONFIDENTIALITY
- PROJECT
- CONCLUSION

INTRODUCTION TO CYBER SECURITY

- **WHAT IS CYBER SECURITY ?**

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. The goal of cybersecurity is to reduce the risk of cyber attacks on devices and services, and to prevent unauthorized access to personal information .

IMPORTANCE :

Protects against unauthorized access to data and networks, improves recovery time after a breach, protects end users and endpoint devices, ensures regulatory compliance, and supports business continuity.

WHAT IS A CYBER THREAT ?

Cyber threats are risks to personal data, national infrastructure, and safety, posed by attackers ranging from lone cybercriminals to nation-states and terrorist groups, using injection attacks and exploiting digital system weaknesses.

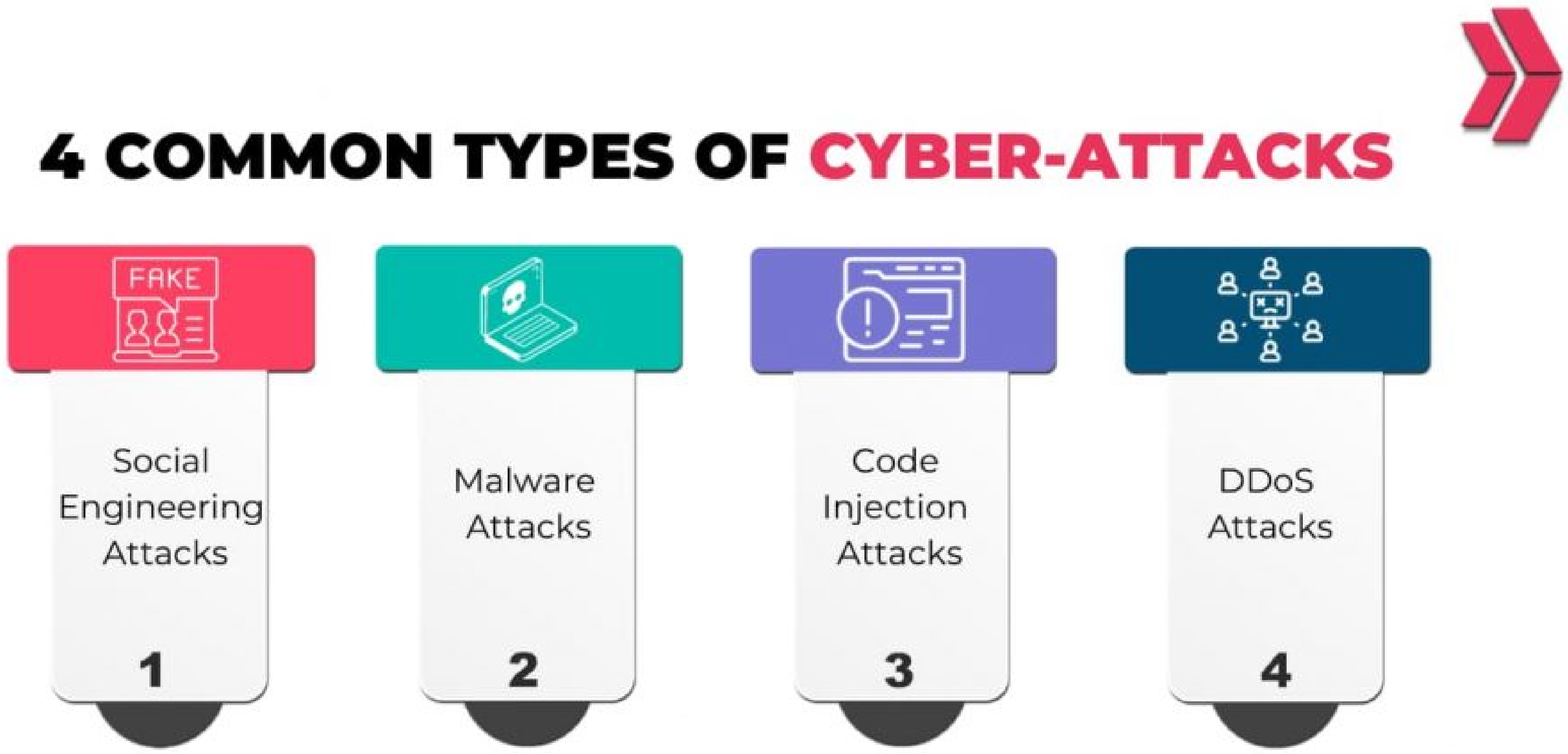
CYBER ATTACK

A cyber attack is a malicious attempt to gain unauthorized access to a computer system or network to cause damage or harm. The goal of a cyber attack is to:

- Disable, disrupt, destroy, or control computer systems
- Alter, block, delete, manipulate, or steal data

TYPES OF CYBER ATTACKS

- Phishing Attack
- Malware Attack
- Code Injection Attack
- Social Engineering
- Spoofing
- MITM (Man In The Middle) Attack
- Etc ..



4 COMMON TYPES OF CYBER-ATTACKS

1. Social Engineering Attacks
2. Malware Attacks
3. Code Injection Attacks
4. DDoS Attacks

INFORMATION CONFIDENTIALITY

Confidentiality of information is the practice of protecting sensitive information from unauthorized access, use, disclosure, modification, loss, or theft.

Information confidentiality can be achieved through following techniques:

- CRYPTOGRAPHY
- STEGANOGRAPHY
- Etc ..

CRYPTOGRAPHY :

Cryptography is the science of secret, or hidden writing .

It has two main Components:

1. Encryption
   - Practice of hiding messages so that they can not be read by anyone other than the intended recipient
2. Authentication & Integrity
   - Ensuring that users of data/resources are the persons they claim to be and that a message has not been surreptitiously altered

CIPHER:

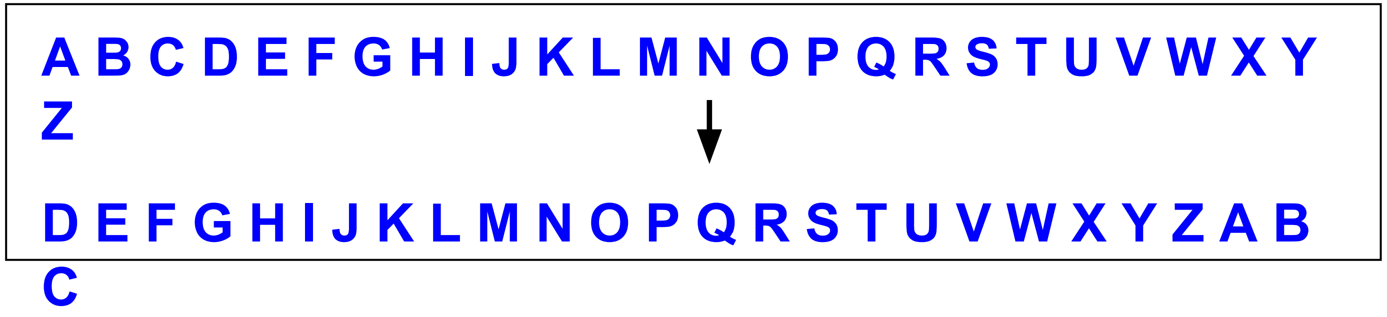
Cipher is a method for encrypting messages .

- The text used to encrypt the original message is called **Cypher Text**

- **Types Encryption :**
  - Symmetric Encryption and
  - Asymmetric Encryption

- **Symmetric Encryption :**

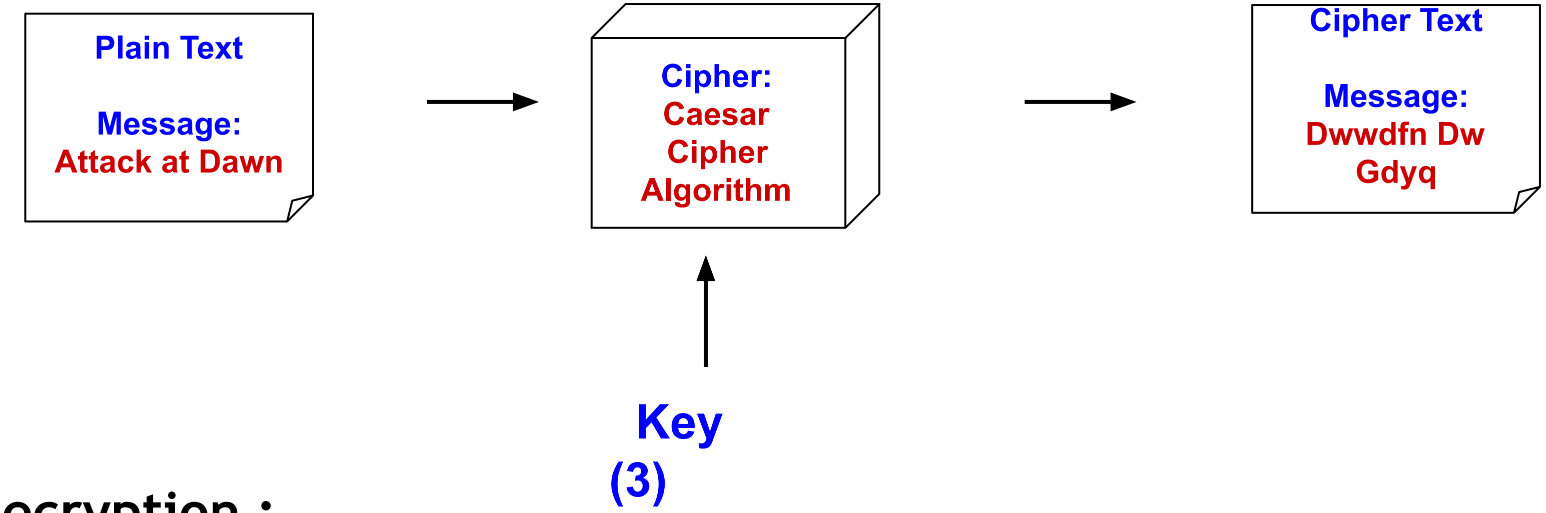
Symmetric encryption is a type of encryption key management solution where only one key (a secret key) is used to both encrypt and decrypt electronic data. The entities communicating via symmetric encryption must exchange the key so that it can be used in the decryption process. i.e , same key is used for encryption and decryption too .



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

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

Encryption :



Plain Text

Message:
Attack at Dawn

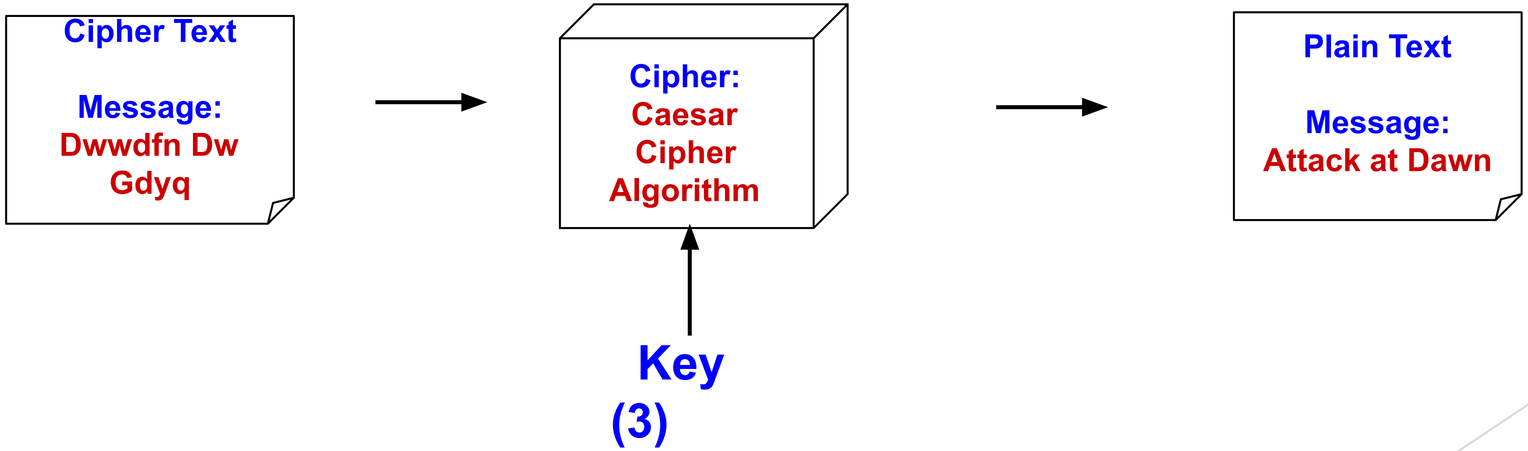
Cipher:
Caesar
Cipher
Algorithm

Cipher Text

Message:
Dwwdfn Dw
Gdyq

Key
(3)

Decryption :



Cipher Text

Message:
Dwwdfn Dw
Gdyq

Cipher:
Caesar
Cipher
Algorithm

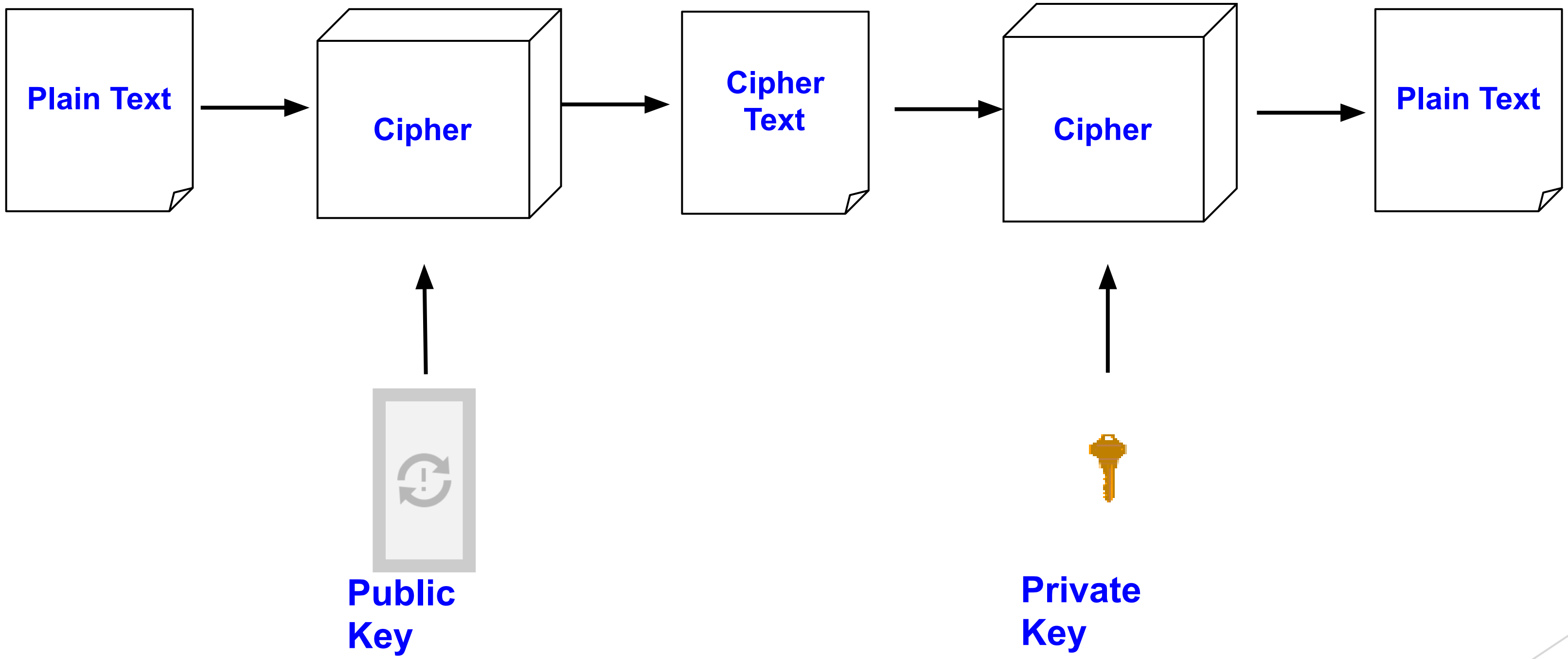
Plain Text

Message:
Attack at Dawn

Key
(3)

- **Asymmetric Encryption :**

Asymmetric encryption is the process of using a public key from a public/private key pair to encrypt plaintext, and then using the corresponding private key to decrypt the ciphertext. Asymmetric encryption relies on asymmetric cryptography, also known as public key cryptography , i.e , messages encoded using public key can only be decoded by the private key .



- **Authentication :**

Authentication in cybersecurity is the process of confirming a user's identity before they can access a computer network or system. It's usually the first step in the cybersecurity process.

Various types of Authentications are :

- **Biometric**
- **Iris matching**
- **Passwords / Credentials**
- **Voice Recognition**
- **Face Recognition**
- **OTP(One Time Password)**

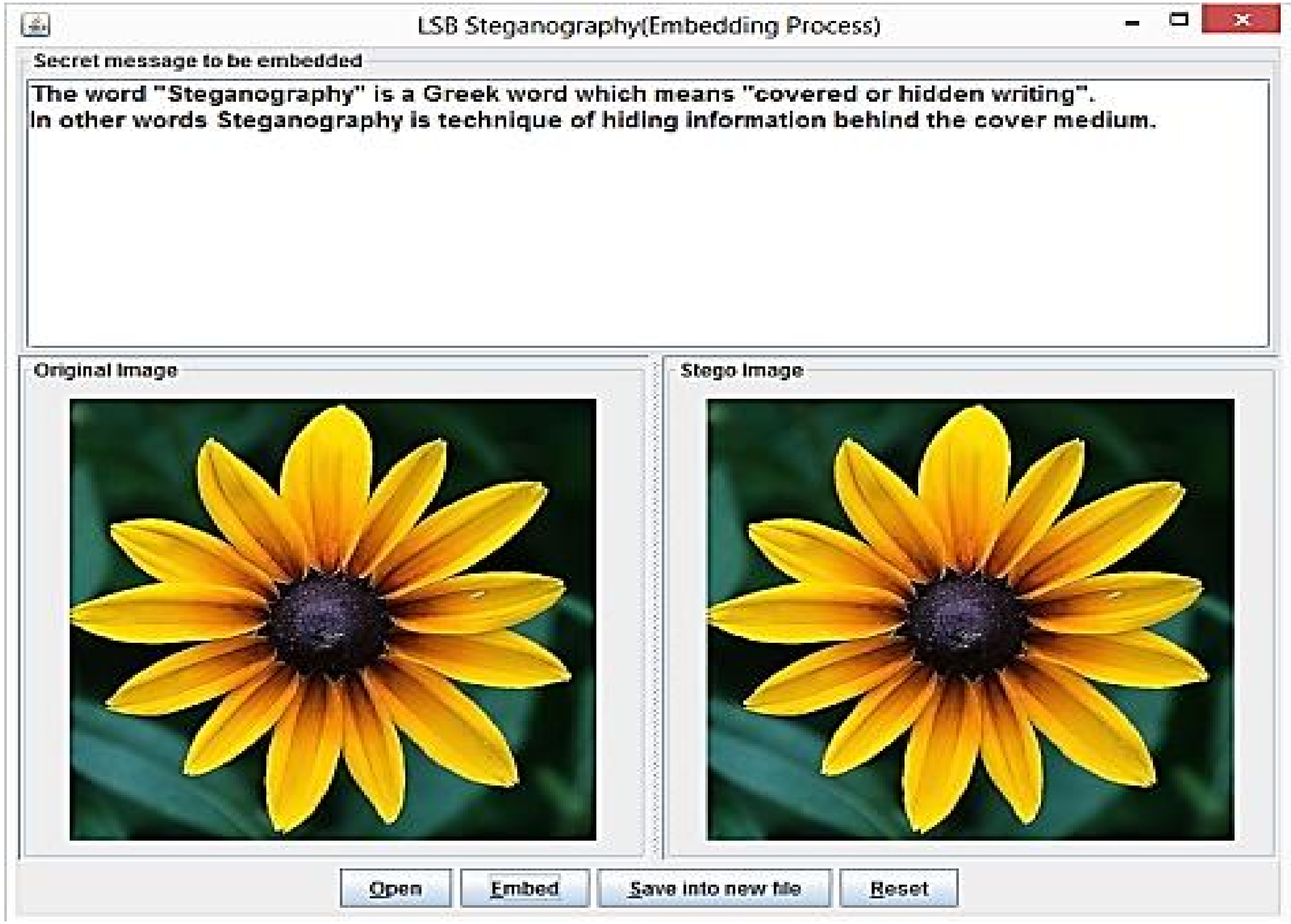
strongdm

- **Steganography :**

Steganography is the practice of concealing information within another message or physical object to avoid detection. Steganography can be used to hide virtually any type of digital content, including text, image, video, or audio content. That hidden data is then extracted at its destination.

Types of steganography :

- Text steganography
- Image steganography
- Video steganography
- Audio steganography



LSB Steganography(Embedding Process)

Secret message to be embedded

The word "Steganography" is a Greek word which means "covered or hidden writing".
In other words Steganography is technique of hiding information behind the cover medium.

Original Image
Stego Image
Open
Embed
Save into new file
Reset

PASSWORD

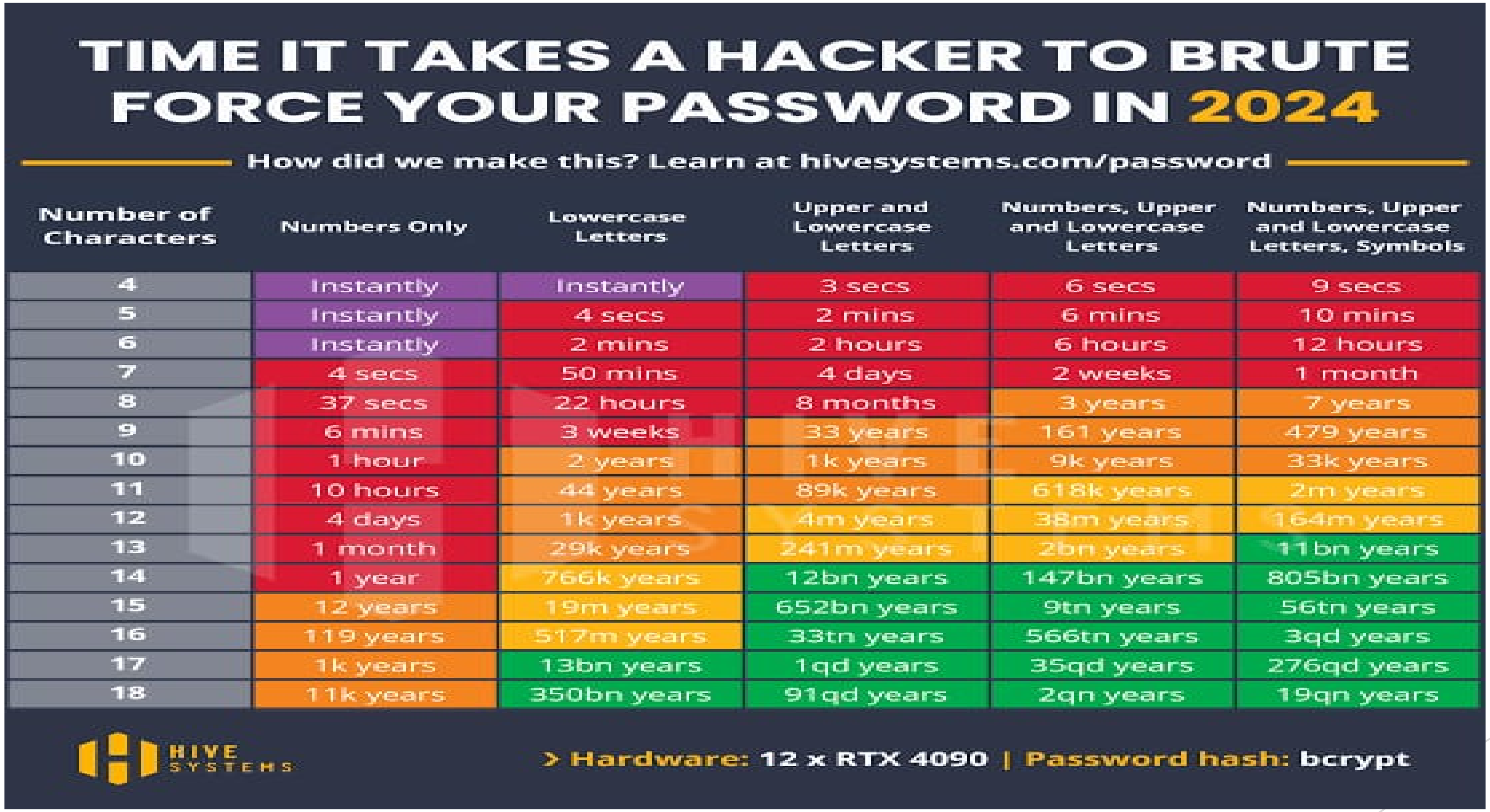
A password is a secret combination of characters(letters, numbers, symbols) used to authenticate a user's identity and grant access to a computer system, network, or digital account.

WHAT MAKES PASSWORD STRONG ?

Minimum eight characters of length highly recommended is twelve characters, more better to contain the special characters like “!@#$%^&*()” and to include combination of upper and lower case characters .

- **STRONG PASSWORD :**
  - **@%12232Rk)***
  - **()*!%*RLqP!12**

- **Weak Password :**
  - Snakes on a plane
  - PASSWORD



TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2024

How did we make this? Learn at hivesystems.com/password

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	3 secs	6 secs	9 secs
5	Instantly	4 secs	2 mins	6 mins	10 mins
6	Instantly	2 mins	2 hours	6 hours	12 hours
7	4 secs	50 mins	4 days	2 weeks	1 month
8	37 secs	22 hours	8 months	3 years	7 years
9	6 mins	3 weeks	33 years	161 years	479 years
10	1 hour	2 years	1k years	9k years	33k years
11	10 hours	44 years	89k years	618k years	2m years
12	4 days	1k years	4m years	38m years	164m years
13	1 month	29k years	241m years	2bn years	11bn years
14	1 year	766k years	12bn years	147bn years	805bn years
15	12 years	19m years	652bn years	9tn years	56tn years
16	119 years	517m years	33tn years	566tn years	3qd years
17	1k years	13bn years	1qd years	35qd years	276qd years
18	11k years	350bn years	91qd years	2qn years	19qn years

HIVE SYSTEMS

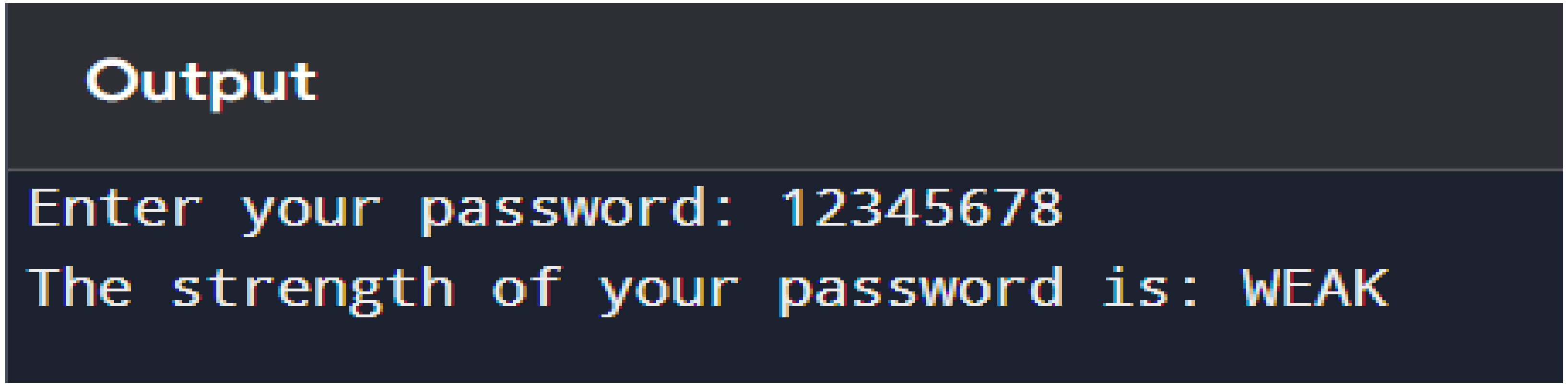
> Hardware: 12 x RTX 4090 | Password hash: bcrypt

Password strength checker code :

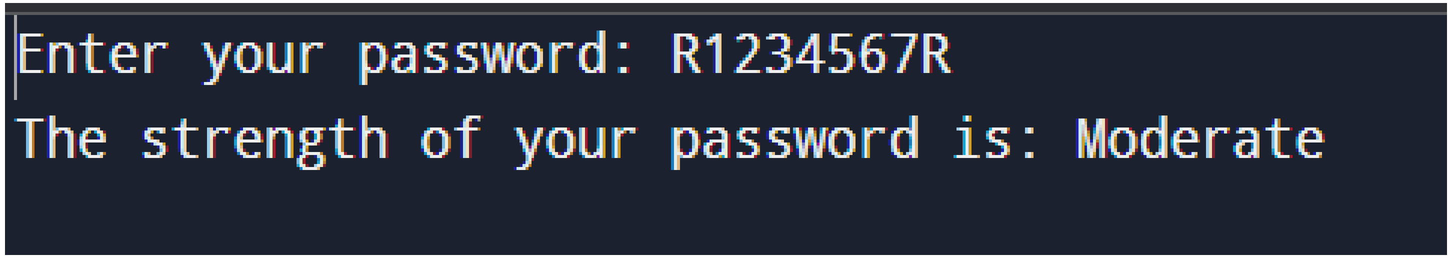
```
def check_password_strength(password):
   if len(password) < 8:
       return "Weak"
   has_upper = any(c.isupper() for c in password)
   has_lower = any(c.islower() for c in password)
   has_digit = any(c.isdigit() for c in password)
   has_special = any(c in '!@#$%^&*()_+-=[]{}|;:,.<>?/~`' for c in password)
   complexity = sum([has_upper, has_lower, has_digit, has_special])
   if complexity == 4:
      return "Very Strong"
   elif complexity == 3:
       return "Strong"
   elif complexity == 2:
      return "Moderate"
```

```
else:
    return "WEAK“
password = input("Enter your password: ")
strength = check_password_strength(password)
print(f"The strength of your password is: {strength}")
```

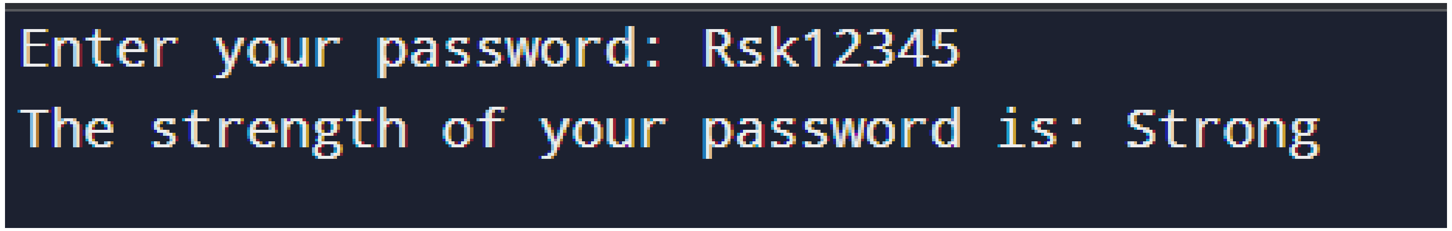
Result :



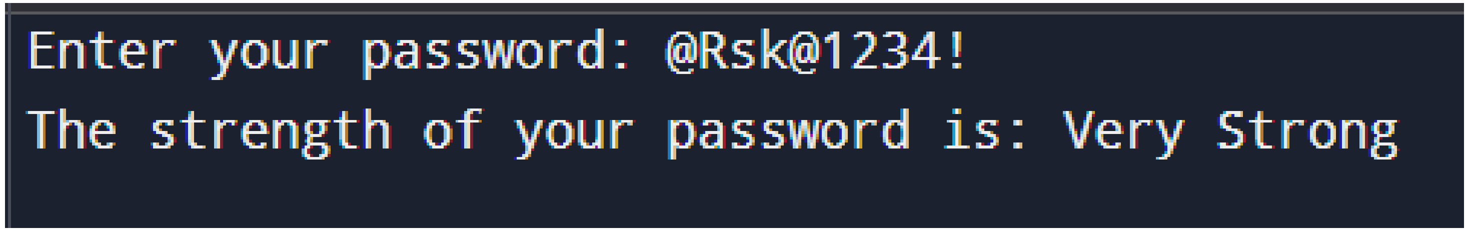
```
Enter your password: 12345678
The strength of your password is: WEAK
```



```
Enter your password: R1234567R
The strength of your password is: Moderate
```



```
Enter your password: Rsk12345
The strength of your password is: Strong
```



```
Enter your password: @Rsk@1234!
The strength of your password is: Very Strong
```

CONCLUSION

Hope my presentation gave some knowledge for how to protect our systems from the cyber attacks and how your passwords should be managed for making your systems safe and free of attacks .

THANK YOU