LectureMaterial#1

Information Security

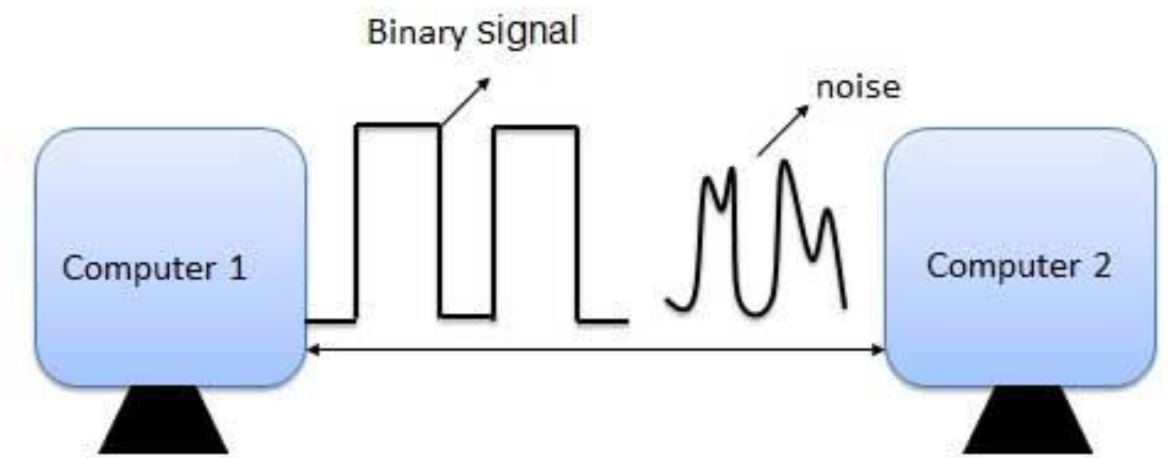
Dr. Abu Nowshed Chy

Department of Computer Science and Engineering

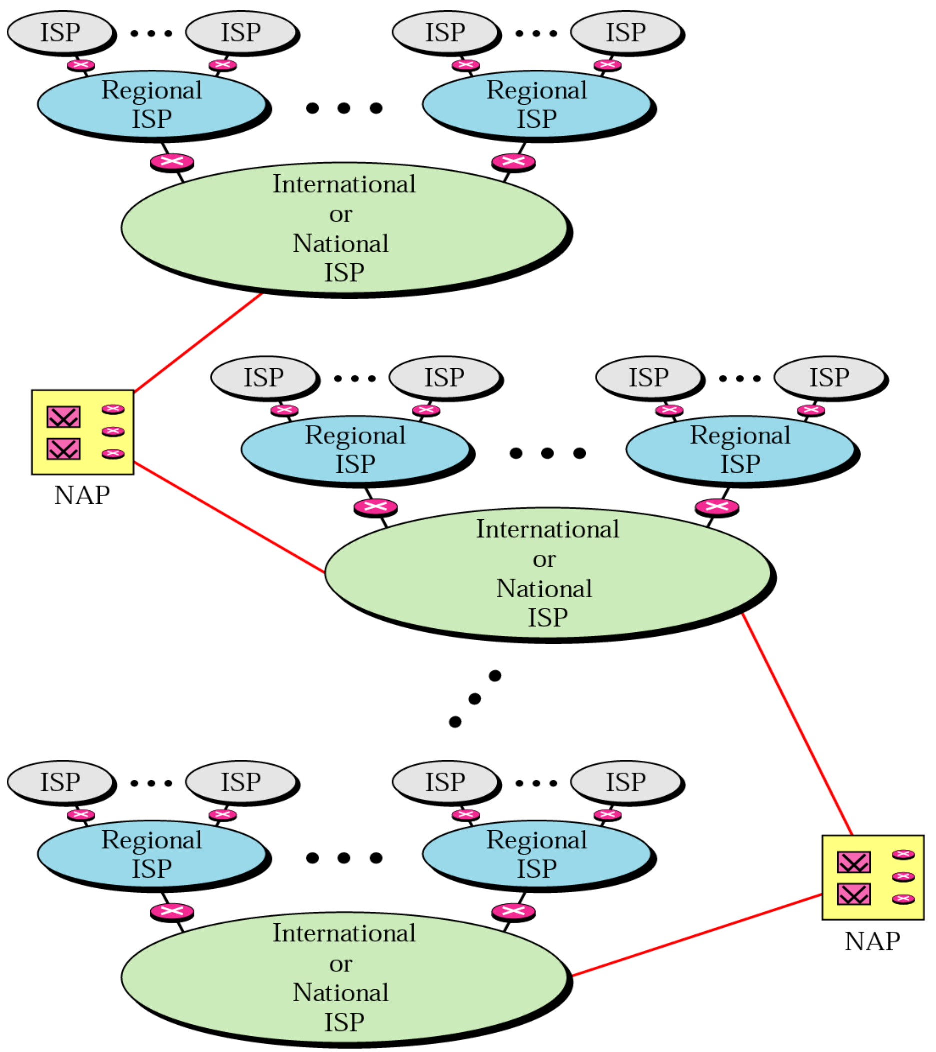
University of Chittagong

Faculty Profile

Data Transmission



WAN


ISP
ISP
ISP
ISP
Regional ISP
Regional ISP
International or National ISP
NAP
ISP
ISP
ISP
ISP
Regional ISP
Regional ISP
International or National ISP
ISP
ISP
ISP
ISP
Regional ISP
Regional ISP
International or National ISP
NAP

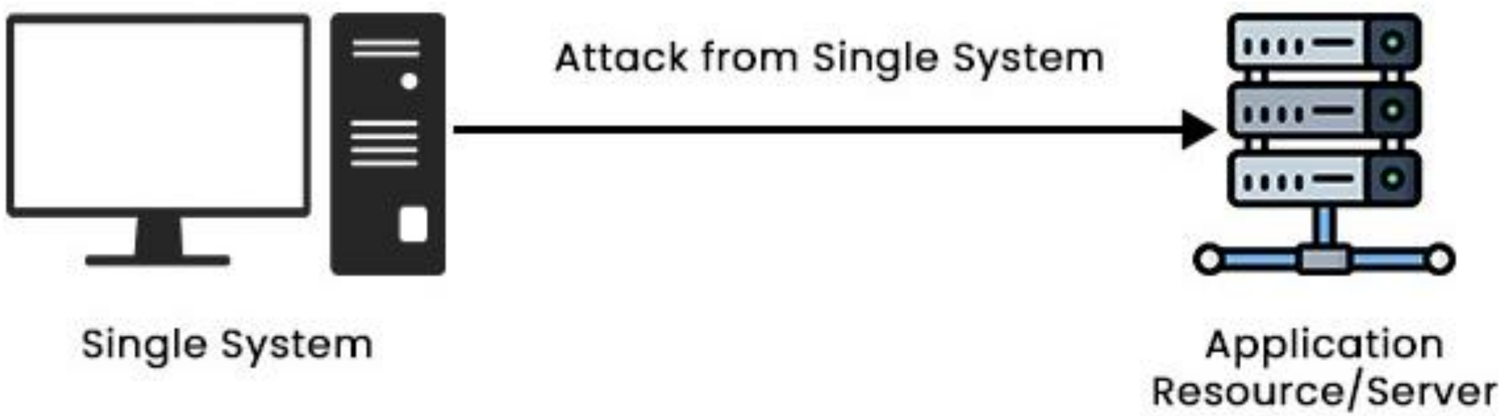
Rogue Security Software

Rogue Security Software

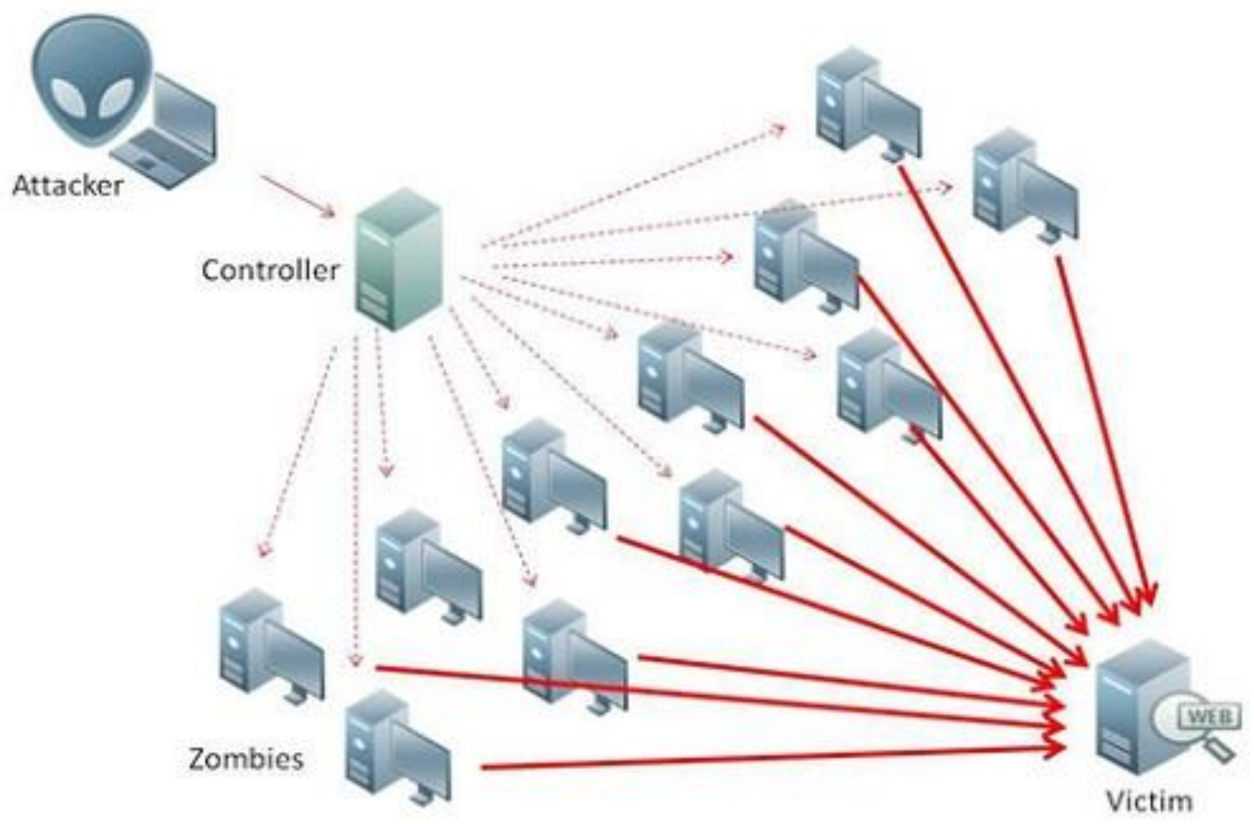
Leveraging the fear of computer viruses, scammers have a found a new way to commit Internet fraud.

Rogue security software is malicious software that mislead users to believe that they have network security issues, most commonly a computer virus installed on their computer or that their security measures are not up to date. Then they offer to install or update users' security settings. They'll either ask you to download their program to remove the alleged viruses, or to pay for a tool. Both cases lead to actual malware being installed on your computer.

DOS Attack


Attack from Single System
Single System
Application
Resource/Server

DDOS Attack



DOS and DDOS Attack

There are cases whenever a website's server gets overloaded with traffic and simply crashes, e.g. sometimes when a news story breaks. But more commonly, this is what happens to a website during a DoS attack, or denial-of-service, a malicious traffic overload that occurs when attackers over-flood a website with traffic. When a website has too much traffic, it's unable to serve its content to visitors.

A DoS attack is performed by one machine and its internet connection, by flooding a website with packets and making it impossible for legitimate users to access the content of flooded website. Fortunately, you can't really overload a server with a single other server or a PC anymore. In the past years it hasn't been that common if anything, then by flaws in the protocol.

DOS and DDOS Attack

A DDoS attack, or distributed denial-of-service attack, is similar to DoS, but is more forceful. It’s harder to overcome a DDoS attack. It’s launched from several computers, and the number of computers involved can range from just a couple of them to thousands or even more.

Since it’s likely that not all of those machines belong to the attacker, they are compromised and added to the attacker’s network by malware. These computers can be distributed around the entire globe, and that network of compromised computers is called botnet.

Since the attack comes from so many different IP addresses simultaneously, a DDoS attack is much more difficult for the victim to locate and defend against.

Phishing

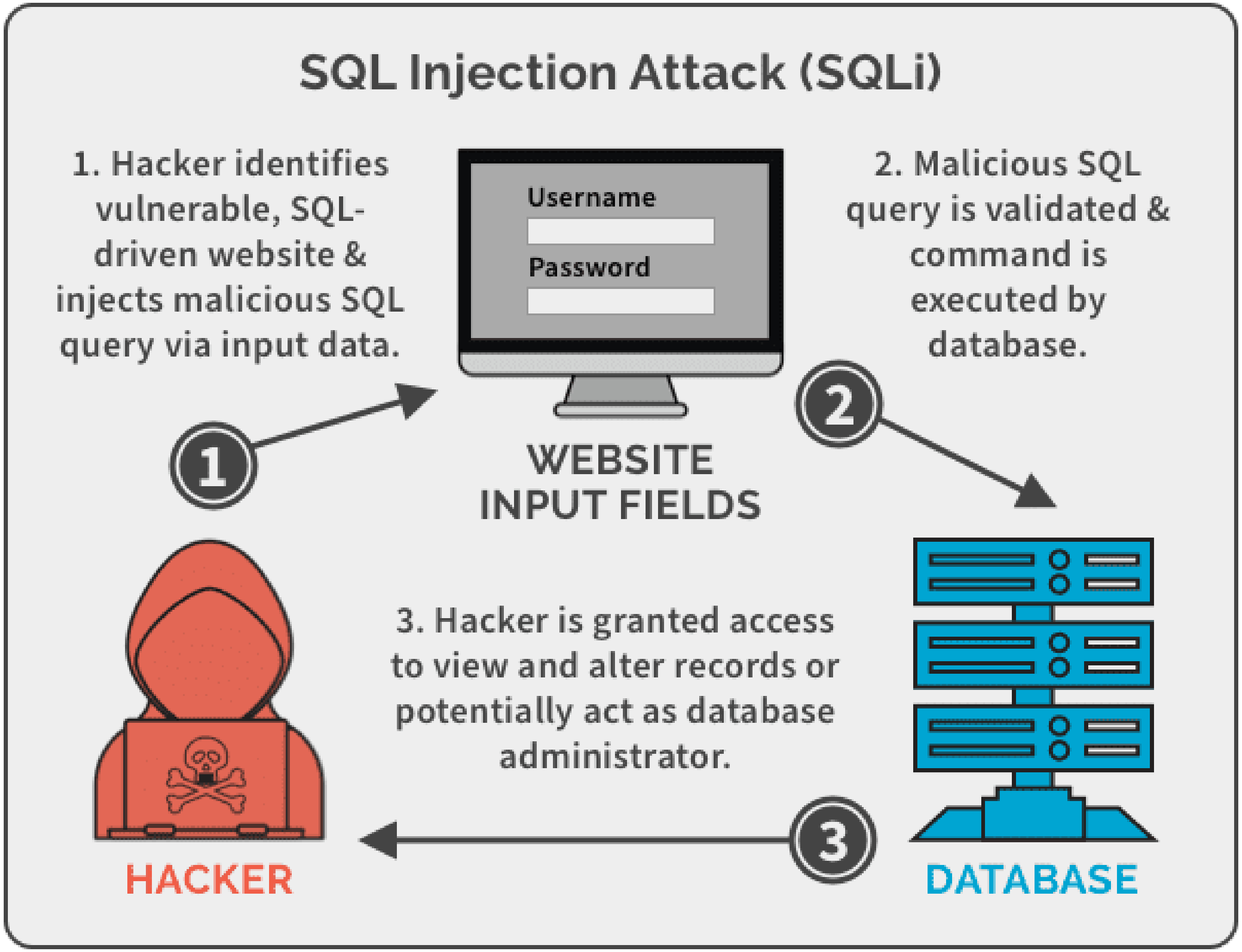
1.
Attacker sends phishing mail to target
Hacker
Target
2.
Victim clicks on Phishing link and visits fake website
3.
Hacker collects important credentials
4.
Hacker uses victim's credentials to access private information
Original Website
Phishing Website

Phishing

Phishing is a method of a social engineering with the goal of obtaining sensitive data such as passwords, usernames, and credit card numbers.

The attacks often come in the form of instant messages or phishing emails designed to appear legitimate. The recipient of the email is then tricked into opening a malicious link, which leads to the installation of malware on the recipient’s computer. It can also obtain personal information by sending an email that appears to be sent from a bank, asking to verify your identity by giving away your private information.

SQL Injection Attack



SQL Injection Attack

```
txtUserId = getRequestString("UserId");
txtSQL = "SELECT * FROM Users WHERE UserId = " + txtUserId;
```

UserId: 105 OR 1=1

```
SELECT * FROM Users WHERE UserId = 105 OR 1=1;
```

SQL Injection Attack

SQL injection attacks are designed to target data-driven applications by exploiting security vulnerabilities in the application's software. They use malicious code to obtain private data, change and even destroy that data, and can go as far as to void transactions on websites. It has quickly become one of the most dangerous privacy issues for data confidentiality.

Clop Ransomware

ClopReadMe.txt - Notepad

File Edit Format View Help

Your network has been penetrated.
All files on each host in the network have been encrypted with a strong algorithm.
Backups were either encrypted or deleted or backup disks were formatted.
Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover
We exclusively have decryption software for your situation
No decryption software is available in the public.
DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME OR MOVE the encrypted and readme files.
DO NOT DELETE readme files.
This may lead to the impossibility of recovery of the certain files.
Photorec, RannohDecryptor etc. repair tools are useless and can destroy your files irreversibly.
If you want to restore your files write to emails (contacts are at the bottom of the sheet) and
(Less than 5 Mb each, non-archived and your files should not contain valuable information
(Databases, backups, large excel sheets, etc.)).
You will receive decrypted samples and our conditions how to get the decoder.

Attention!!!
Your warranty - decrypted samples.
Do not rename encrypted files.
Do not try to decrypt your data using third party software.
We don`t need your files and your information.

But after 2 weeks all your files and keys will be deleted automatically.
Contact emails:
servicedigilogos@protonmail.com
or
managersmaers@tutanota.com

The final price depends on how fast you write to us.

Clop

Clop Ransomware

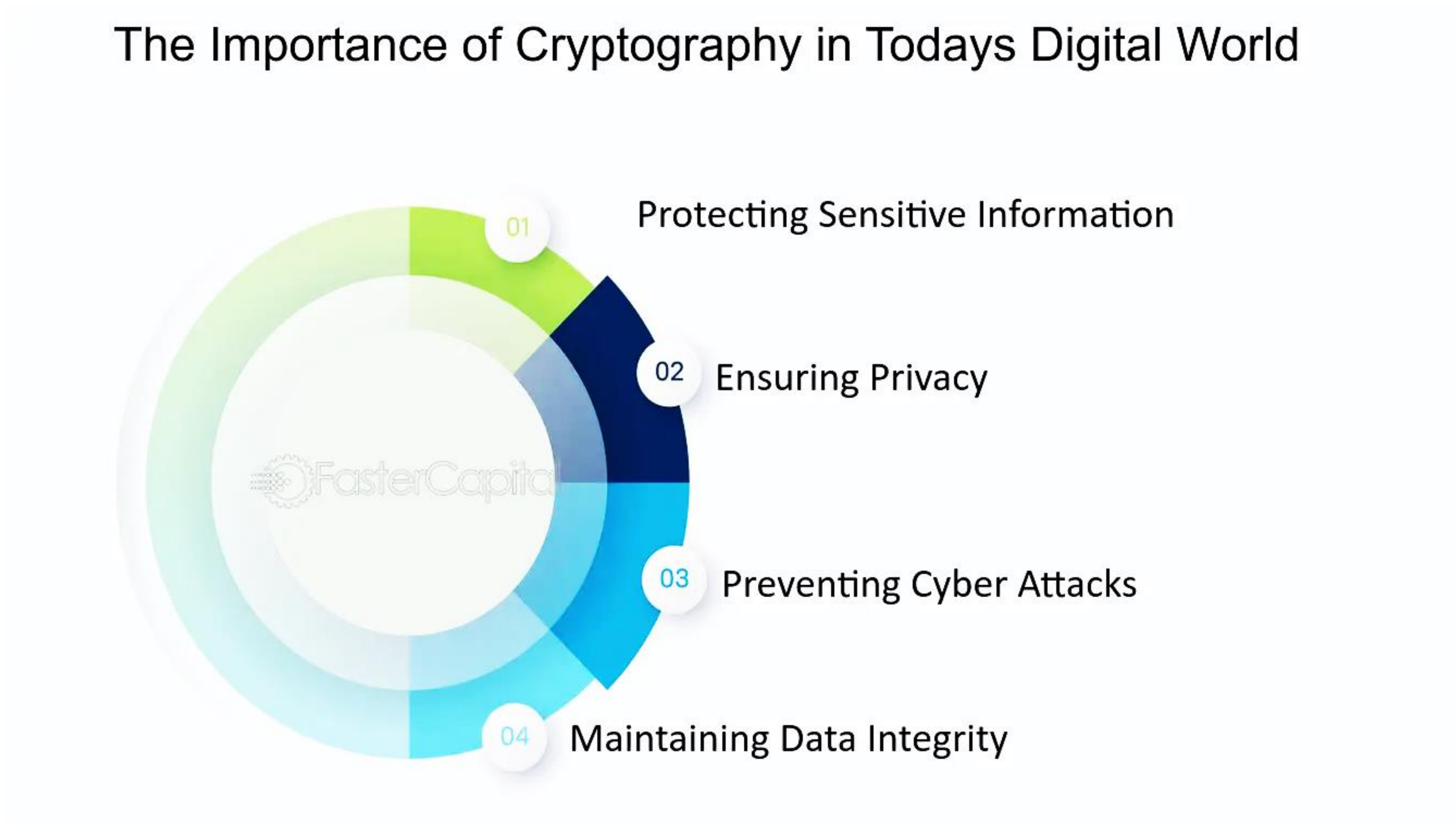
Ransomware is malware which encrypts your files until you pay a ransom to the hackers. “Clop” is one of the latest and most dangerous ransomware threats. It’s a variant of the well-known CryptoMix ransomware, which frequently targets Windows users.

Before beginning the encryption process, the Clop ransomware blocks over 600 Windows processes and disables multiple Windows 10 applications, including Windows Defender and Microsoft Security Essentials — leaving you with zero chance of protecting your data.

The Clop ransomware has evolved since its inception, now targeting entire networks — not just individual devices. Even the Maastricht University in the Netherlands became a victim of the Clop ransomware, with almost all Windows devices on the university’s network being encrypted and forced to pay a ransom.

What are the Solutions!!!!

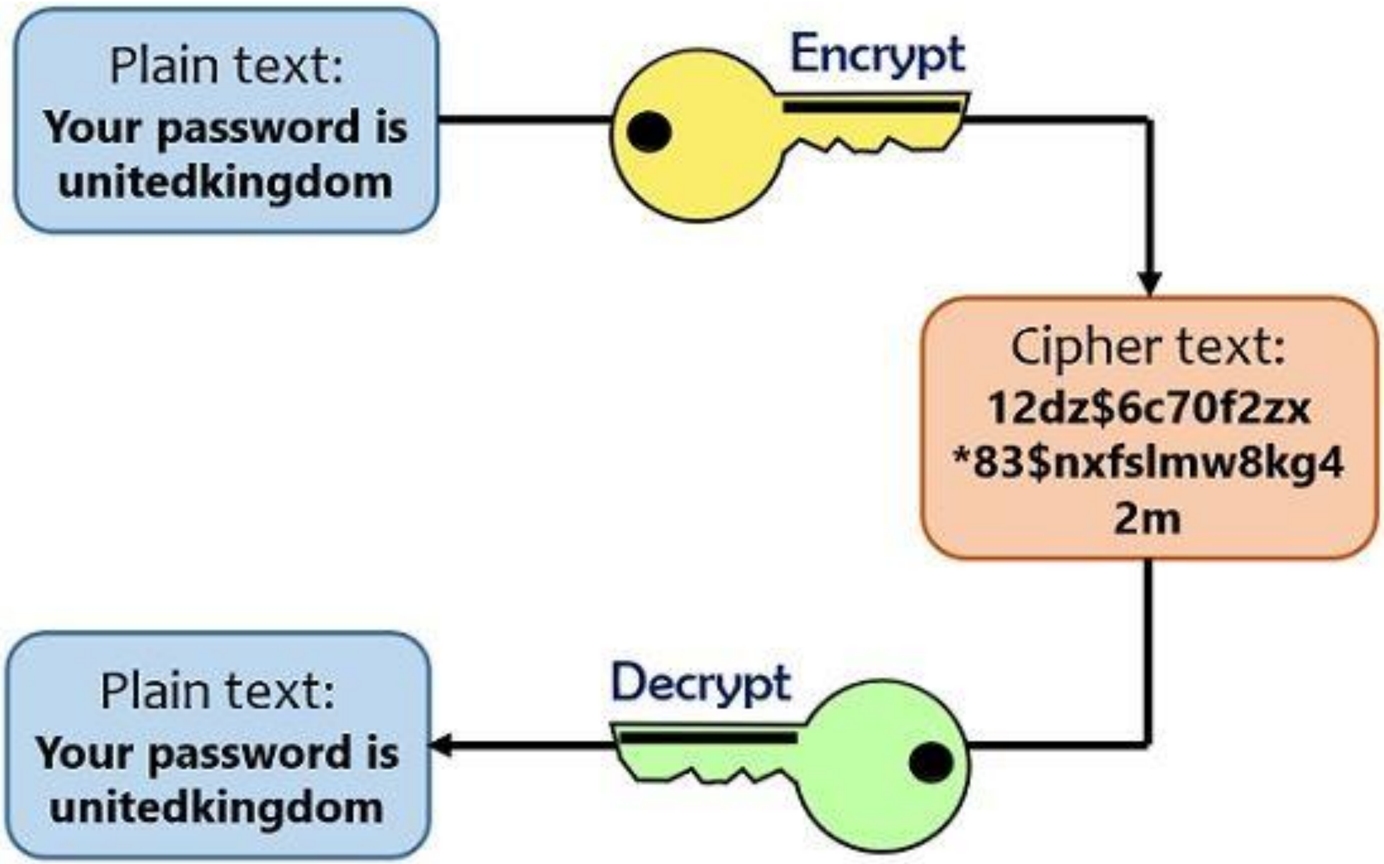
Importance of Cryptography



Cryptography

- Cryptography is the mathematical "scrambling" of data so that only someone with the necessary key can "unscramble" it.
- Cryptography allows secure transmission of private information over insecure channels (for example packet switched networks).
- Cryptography also allows secure storage of sensitive data on any computer.

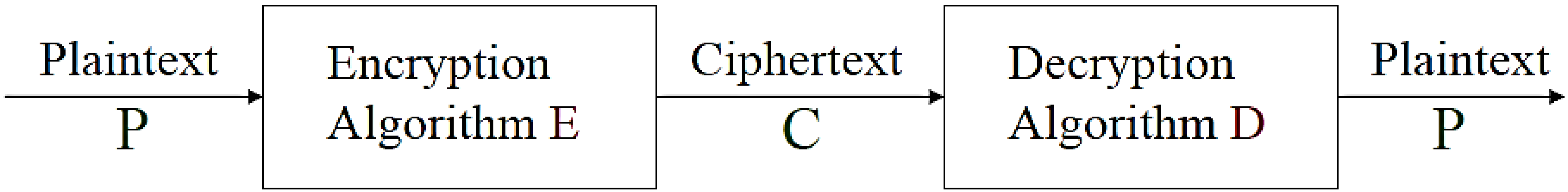
Cryptography



Common Terms in Cryptography

In cryptography, *encryption* is the process of transforming information (referred to as *plaintext*) using an algorithm (called *cipher*) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a *key*. The result of the process is encrypted information (in cryptography, referred to as *ciphertext*). In many contexts, the word encryption also implicitly refers to the reverse process, *decryption*, to make the encrypted information readable again (i.e. to make it unencrypted).

Cryptosystem

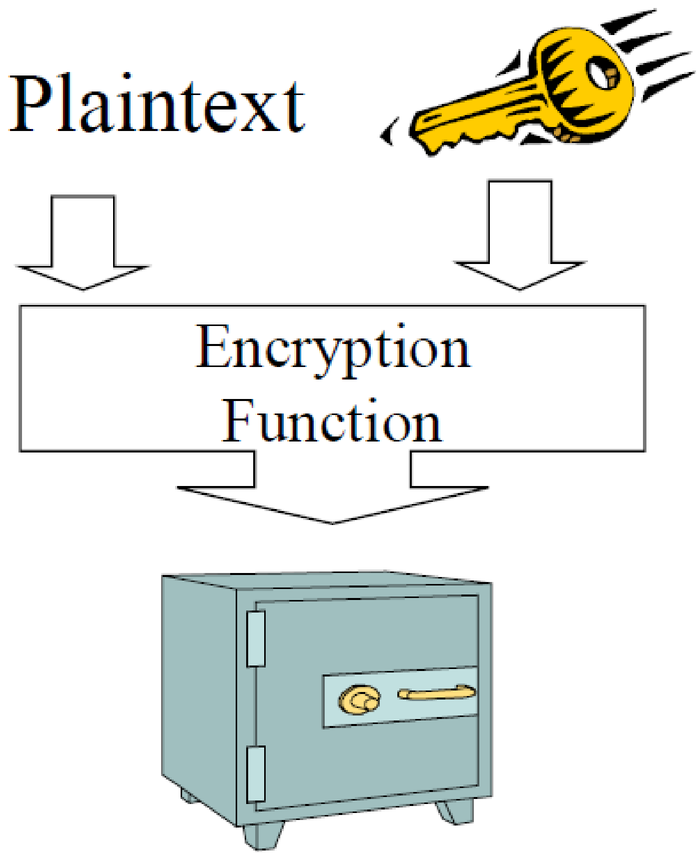


- Algorithm: a set of rules
- Algorithm often uses a parameter – key K
  - Key provides flexibility
  - Same algorithm can be used by different users with different keys
  - Security depends on the secret key value while algorithm can be public

Encryption

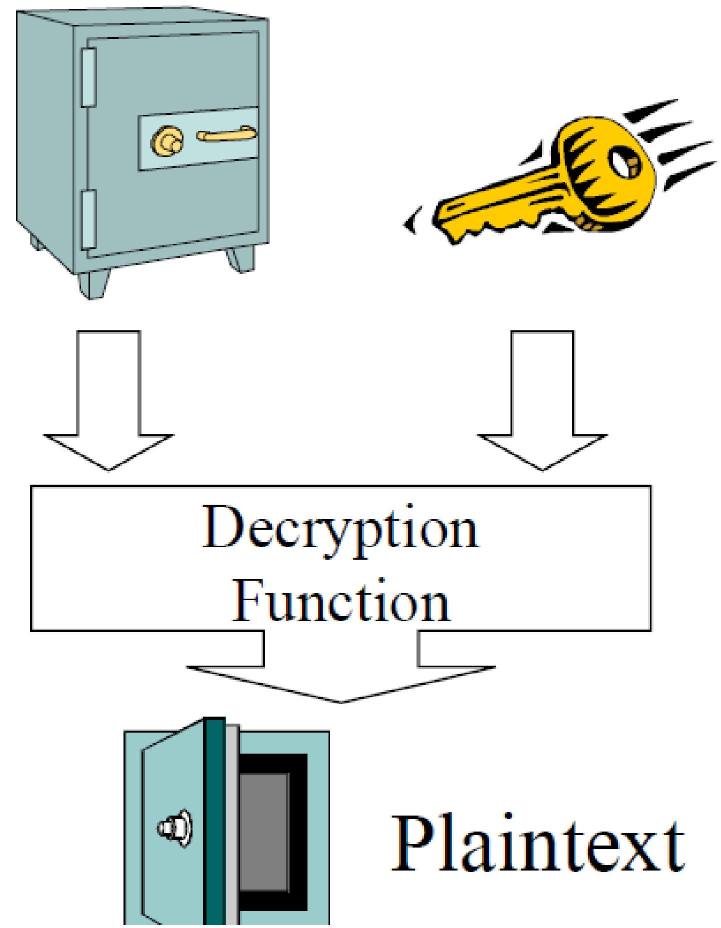
- Encryption is the process of feeding plaintext and key into a function and getting ciphertext output

- Ciphertext is “garbage” unless decrypted



Decryption

- Decryption is the process of feeding ciphertext and a key into another function and getting original plaintext output



Common Cryptography Techniques!!!!

Modular Arithmetic

If a and b are integers with $a \neq 0$, we say that a *divides* b if there is an integer c such that $b = ac$. When a divides b we say that a is a *factor* of b and that b is a *multiple* of a. The notation $a \mid b$ denotes that a divides b. We write $a \nmid b$ when a does not divide b.

Determine whether $3 \mid 7$ and whether $3 \mid 12$.

Modular Arithmetic

Let a, b, and c be integers. Then

(i) if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;

(ii) if $a \mid b$, then $a \mid bc$ for all integers c;

(iii) if $a \mid b$ and $b \mid c$, then $a \mid c$.

Modular Arithmetic

THE DIVISION ALGORITHM Let a be an integer and d a positive integer. Then there are unique integers q and r, with $0 \leq r < d$, such that $\boxed{a = dq + r}$.

In the equality given in the division algorithm, d is called the *divisor*, a is called the *dividend*, q is called the *quotient*, and r is called the *remainder*. This notation is used to express the quotient and remainder:

$$q = a \textbf{ div } d, \quad r = a \textbf{ mod } d.$$

What are the quotient and remainder when 101 is divided by 11?

What are the quotient and remainder when -11 is divided by 3?

Caesar Cipher Encryption

To express Caesar's encryption process mathematically, first replace each letter by an integer from 0 to 25, based on its position in the alphabet. For example, replace A by 0, K by 10, and Z by 25. Caesar's encryption method can be represented by the function f that assigns to the nonnegative integer p, $p \leq 25$, the integer $f(p)$ in the set $\{0, 1, 2, \ldots, 25\}$ with

$$f(p) = (p + 3) \textbf{ mod } 26.$$

A = 0	B = 1	C = 2	D = 3	E = 4	F = 5	G = 6	H = 7	I = 8	J = 9
K = 10	L = 11	M = 12	N = 13	O = 14	P = 15	Q = 16	R = 17	S = 18	T = 19
U = 20	V = 21	W = 22	X = 23	Y = 24	Z = 25				

Caesar Cipher Encryption

A = 0	B = 1	C = 2	D = 3	E = 4	F = 5	G = 6	H = 7	I = 8	J = 9
K = 10	L = 11	M = 12	N = 13	O = 14	P = 15	Q = 16	R = 17	S = 18	T = 19
U = 20	V = 21	W = 22	X = 23	Y = 24	Z = 25				

What letter replaces the letter K when the function $f(p) = (7p + 3) \bmod 26$ is used for encryption?

Caesar Cipher Decryption

$$f^{-1}(p) = (p - k)\ \mathbf{mod}\ 26.$$

Decrypt the ciphertext message “PBZOBQ” that was encrypted using the Caesar cipher encryption technique with shift k = -3.

A = 0	B = 1	C = 2	D = 3	E = 4	F = 5	G = 6	H = 7	I = 8	J = 9
K = 10	L = 11	M = 12	N = 13	O = 14	P = 15	Q = 16	R = 17	S = 18	T = 19
U = 20	V = 21	W = 22	X = 23	Y = 24	Z = 25				

Caesar Cipher Decryption

What is the secret message produced from the message "CSECU" using the Caesar cipher with the encryption function $f(p) = (p + 12) \bmod 26$?

Decrypt the ciphertext message "CHATTOGRAM" that was encrypted using the Caesar cipher encryption technique with shift k = 7.

A = 0	B = 1	C = 2	D = 3	E = 4	F = 5	G = 6	H = 7	I = 8	J = 9
K = 10	L = 11	M = 12	N = 13	O = 14	P = 15	Q = 16	R = 17	S = 18	T = 19
U = 20	V = 21	W = 22	X = 23	Y = 24	Z = 25				

Playfair Cipher

Playfair Cipher

Step 1: Choose Key phrase for the Encryption of your Plain text.

Let’s say we want to encrypt the plain text “HELLO WORLD” using the key phrase “SECURITY”.

When choosing a term, make sure that no letter is duplicated, and especially that the letters I and J do not appear together. Keywords like INJURE, JUICE, and JIGSAW, for example, would be disqualified since they feature both I and J at the same time, which violates this criteria.

Playfair Cipher

Step 2: Now create 5 X 5 Playfair Matrix or Key Matrix according to your Key.

S	E	C	U	R
I	T	Y		

Playfair Cipher

The remaining squares of the matrix are then filled with the remaining alphabet letters, in alphabetical sequence. However, since there are 26 letters and only 25 squares available, we allocate both I and J to the same square.

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

Playfair Cipher

Step 3: Preparing the Message

The next step is to prepare the message for encryption. We remove any non-alphabetic characters and convert all letters to uppercase. In our example, the message “HELLO WORLD” becomes “HELLOWORLD”.

Playfair Cipher

Step 4: Breaking the Message into Pairs. (Making digraphs of Plaintext)

To encrypt the message using the Playfair cipher, we break the message into pairs of letters. If we have an odd number of letters, we usually add a placeholder letter (e.g., “X”) at the end to create a pair. If in between duplicate letters come in same pair then we will break it into single letter and attach X at the first letter then will start making the other pairs.

“HELLOWORLD”

Playfair Cipher

Step 5: Now take one pair at a time and look for it in the key matrix.

There are mainly three criteria for encrypting letters.

#1: If the two letters in the pair are in the same row of the key square, we replace them with the letter to their right.

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

Playfair Cipher

#2: If both letters in the pair are found in the same column of the key square, we will replace each letter with the letter below it.

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

Playfair Cipher

#2: If both letters in the pair are found in the same column of the key square, we will replace each letter with the letter below it.

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

DE

Shape: Column
Rule: Pick Items Below Each Letter, Wrap to Top if Needed

OD

Playfair Cipher

#3: If the letters are in different rows and columns, we form a rectangle with them and change each letter with the letter in the opposite corner. Let suppose we have to find encrypted text for N and T.

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

Playfair Cipher

#3: If the letters are in different rows and columns, we form a rectangle with them and change each letter with the letter in the opposite corner. Let suppose we have to find encrypted text for N and T.

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

Playfair Cipher

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

"HELLOWORLD"

"HE | LX | LO | WO | RL | DX".

"FU | OQ | MP | XN | SP | HQ".

Playfair Cipher (Practice Example)

Let's say we want to encrypt the plain text "HELLO WORLD" using the key phrase "KEYWORD."

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

Playfair Cipher (Practice Example)

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

"HELLOWORLD"

"HE | LX | LO | WO | RL | DX"

"GY | JZ | SC | OK | CF | BU"

Playfair Cipher (Practice Example)

Using the following Playfair matrix, encrypt the following message:

See you at CSECU

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

Playfair Cipher (Practice Example)

Let's say we want to decrypt the plain text "gddogdrqprsdhmembv" using the key phrase "Charles".

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


Thank You!