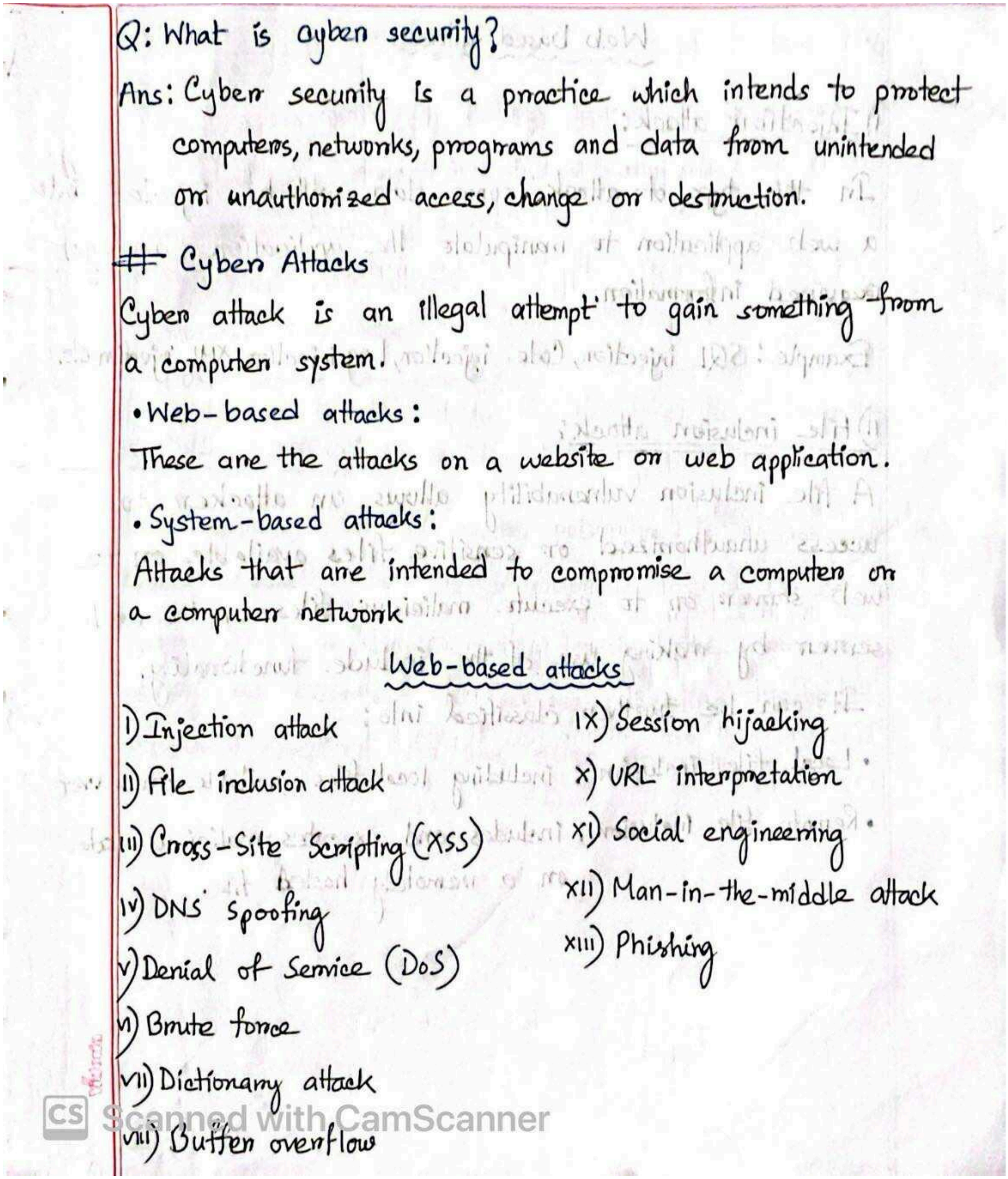
Lecture 1: intruduction.pdf - Google Drive

Lecture 2: Types of cyber attack



Q: What is cyber security?

Ans: Cyber security is a practice which intends to protect computers, networks, programs and data from unintended or unauthorized access, change or destruction.

Cyber Attacks

Cyber attack is an illegal attempt to gain something from a computer system.

- Web-based attacks:

These are the attacks on a website or web application.

- System-based attacks:

Attacks that are intended to compromise a computer or a computer network

<u>Web-based attacks</u>

i) Injection attack

ii) File inclusion attack

iii) Cross-Site Scripting (XSS)

iv) DNS Spoofing

v) Denial of Service (DoS)

vi) Brute force

vii) Dictionary attack

viii) Buffer overflow

ix) Session hijacking

x) URL interpretation

xi) Social engineering

xii) Man-in-the-middle attack

xiii) Phishing

Web based attacks

I) Injection attack:

In this type of attack some data will be injected into a web application to manipulate the application and get required information.

Example: SQL injection, Code injection, Log injection, XML injection etc.

II) File inclusion attack:

A file inclusion vulnerability allows an attacker to access unauthorized or sensitive files available on the web server or to execute malicious files on the web server by making use of the include functionality.

It can be further classified into:

- Local file inclusion: including local files available on server.
- Remote file inclusion: includes and executes malicious code on a remotely hasted file.

Date : / /

III) Cross-Site Scripting (XSS) :

This can be done by editing javascript in a webpage such that it will be executed in client browser.

It can be classified into -

- Reflected XSS attack
- Stored XSS attack
- DOM-based XSS attack

IV) DNS Spoofing :

DNS spoofing (or DNS cache poisoning) is a computer hacking attack, whereby data is introduced into a Domain Name System (DNS) resolver's cache causing the name server to return an incorrect IP address, diverting traffic to the attacker's computer (or any other computer)

v) Denial of Service (DoS):

DoS attack is an attempt to make a server or network source unavailable to users. This is generally done by flooding the server with communication requests. DoS uses single system and single internet connection to attack a server.

It can be classified into:

- Volume based attacks

⇒ goal is to saturate the bandwidth of the attacked site and is measured in bits per second.

- Protocal attack

⇒ consumes actual server resources and is measured in packets per sound

- Application layer attacks

⇒ goal of these attacks is to crash the web server & is measured in requests per second.

VI) Brute force:

It is a trial and error method. Generates large number of guesses and validate them to obtain actual data (passwords in general).

VII) Dictionary attack:

Contains a list of commonly used passwords and validate them to get original password.

VIII) Buffer overflow:

Occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold.

IX) Session hijacking:

Web applications uses cookies to store state and details for user sessions. By stealing the cookies, the attacker can have access to all of user data.

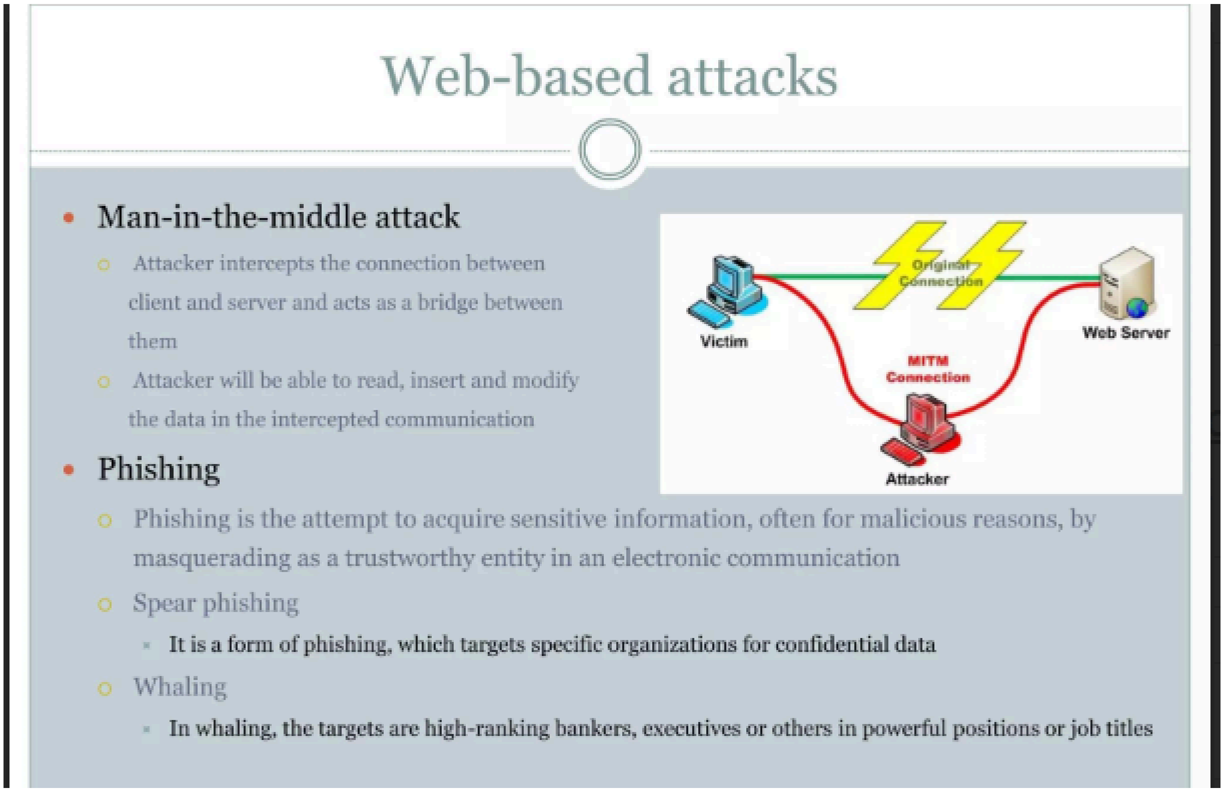
X) URL interpretation:

By changing certain parts of a URL, one can make a web server to deliver web pages for which he is not authorized to browse.

Date : / /

XI) Social Engineering:

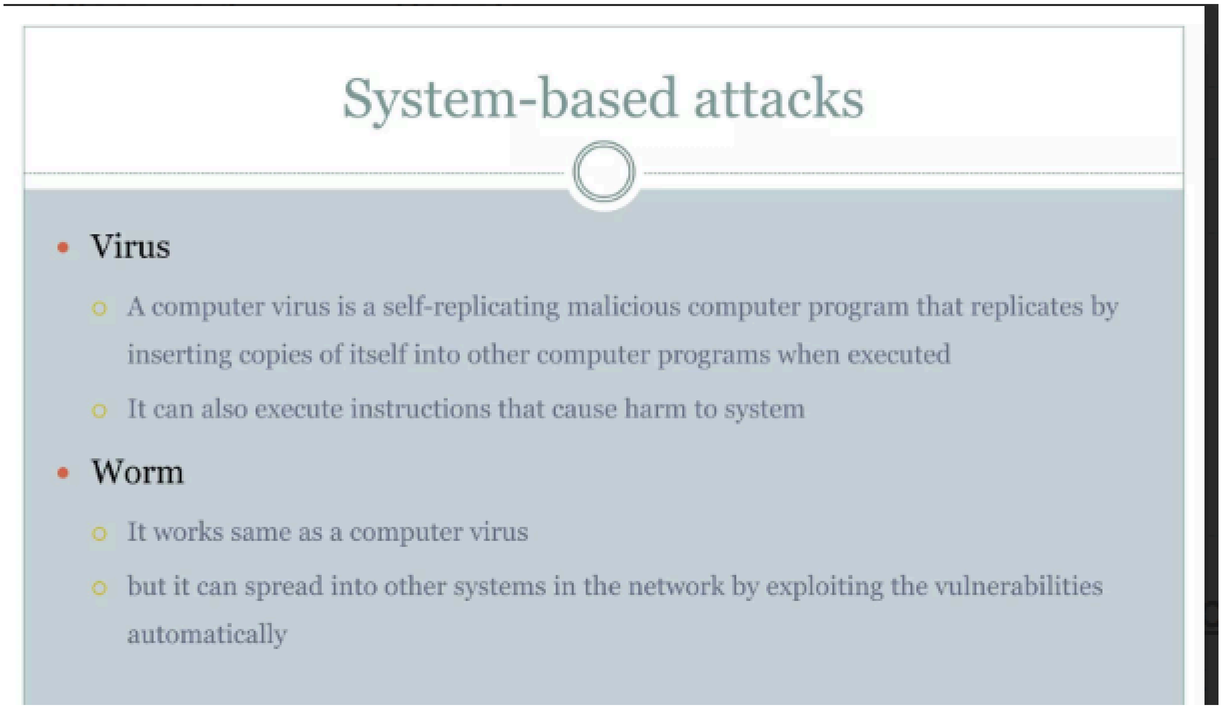
It is a non-technical method that relies heavily on human interaction and often involves tricking people into breaking normal security procedures.



Web-based attacks

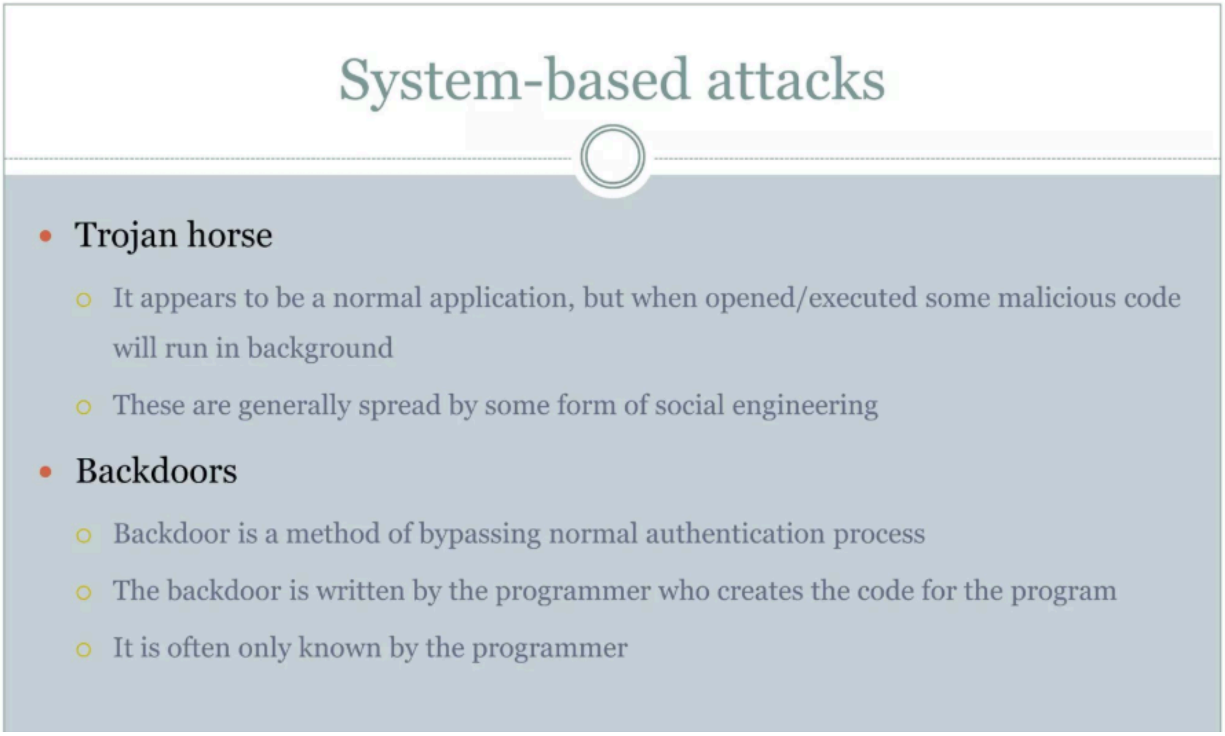
- Man-in-the-middle attack
  - Attacker intercepts the connection between client and server and acts as a bridge between them
  - Attacker will be able to read, insert and modify the data in the intercepted communication

- Phishing
  - Phishing is the attempt to acquire sensitive information, often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication
  - Spear phishing
    - It is a form of phishing, which targets specific organizations for confidential data
  - Whaling
    - In whaling, the targets are high-ranking bankers, executives or others in powerful positions or job titles



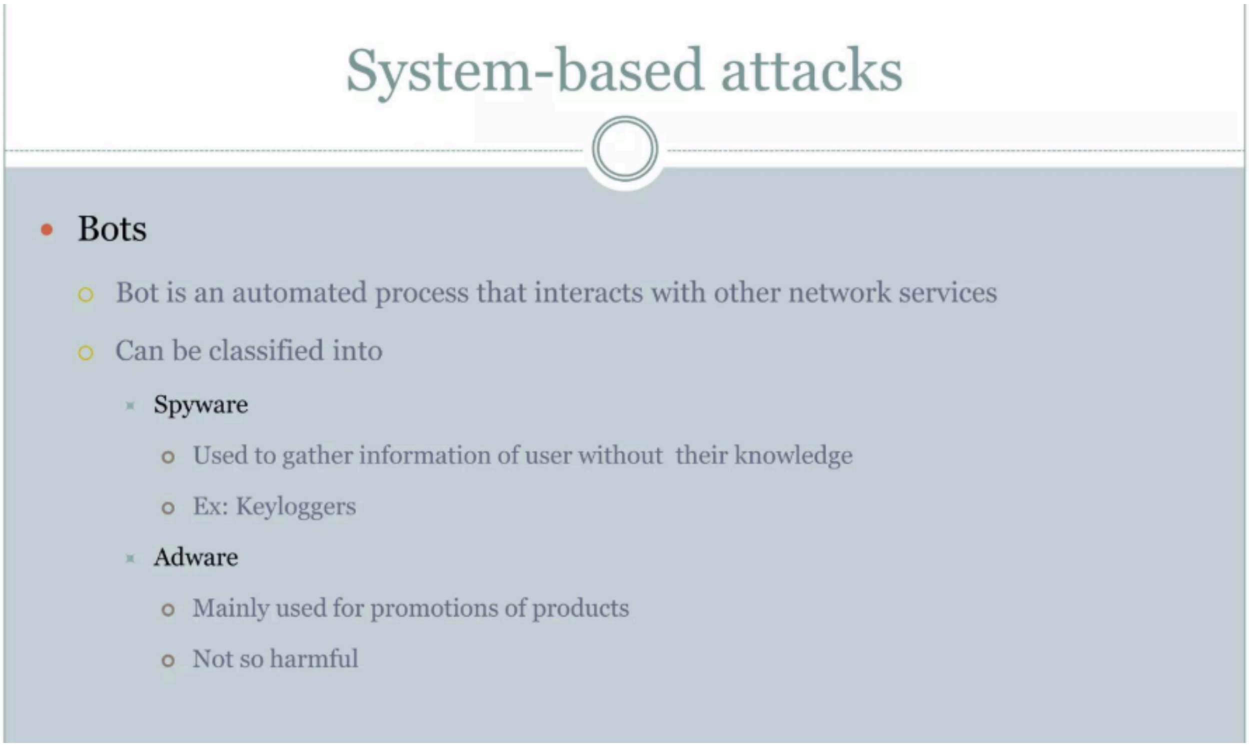
System-based attacks

- Virus
  - A computer virus is a self-replicating malicious computer program that replicates by inserting copies of itself into other computer programs when executed
  - It can also execute instructions that cause harm to system
- Worm
  - It works same as a computer virus
  - but it can spread into other systems in the network by exploiting the vulnerabilities automatically



System-based attacks

- Trojan horse
  - It appears to be a normal application, but when opened/executed some malicious code will run in background
  - These are generally spread by some form of social engineering
- Backdoors
  - Backdoor is a method of bypassing normal authentication process
  - The backdoor is written by the programmer who creates the code for the program
  - It is often only known by the programmer



System-based attacks

- Bots
  - Bot is an automated process that interacts with other network services
  - Can be classified into
    - Spyware
      - Used to gather information of user without their knowledge
      - Ex: Keyloggers
    - Adware
      - Mainly used for promotions of products
      - Not so harmful

Methods to assist in cyberattacks

- Spoofing
  - In spoofing, one person successfully impersonates as another by falsifying the data
  - Ex: IP spoofing, email spoofing etc.,
- Sniffing
  - Sniffing a process of capturing and analyzing the traffic in a network
- Port scanning
  - It is a method to probe a system for open ports
  - Intruder can exploit the vulnerabilities of open ports

CSE 317

Computer & Cyber Security

Date : 25 / 7 / 25

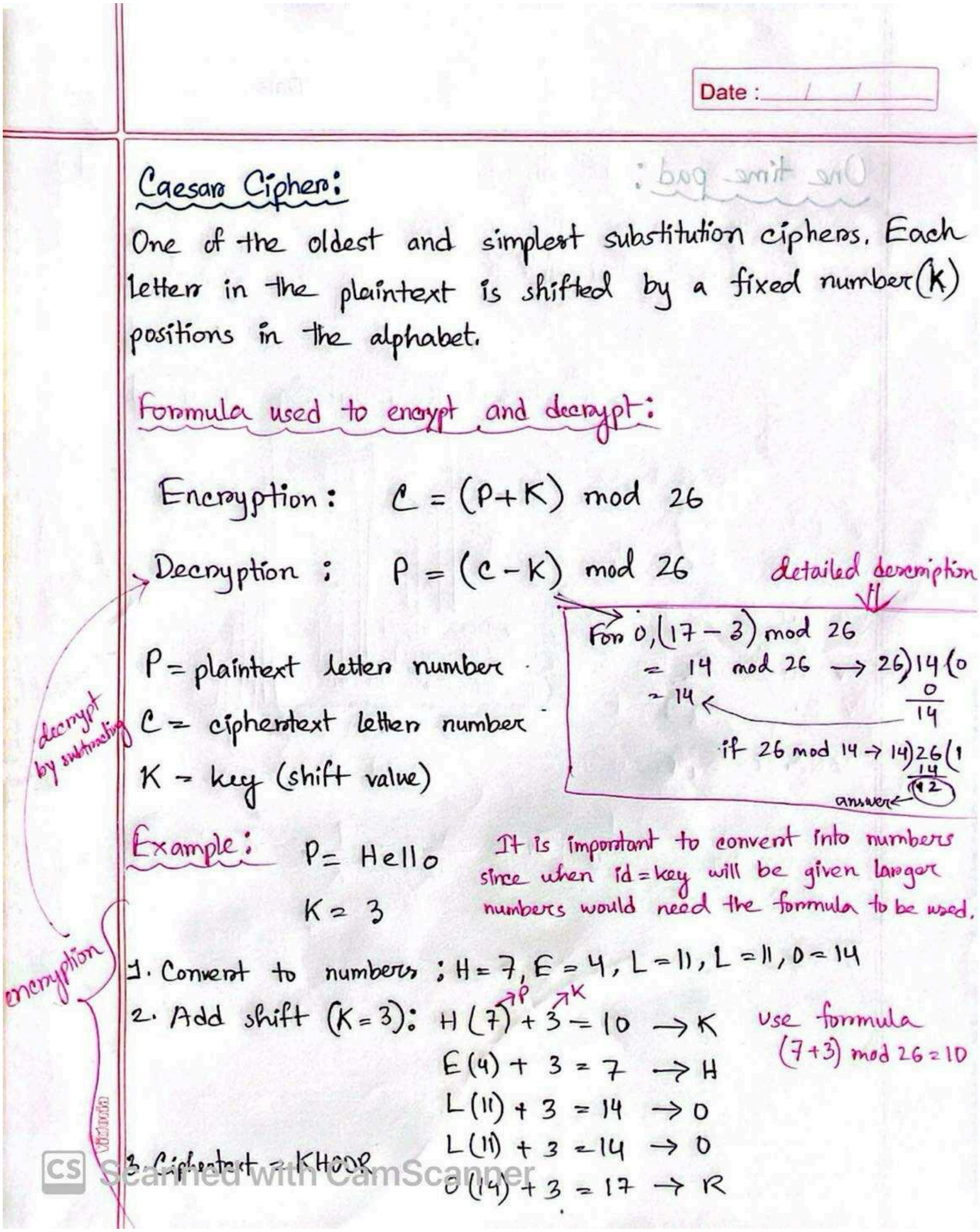
Cyber Attack	Description	Mitigation Techniques
Phishing	Deceptive email / websites trick users into revealing sensitive information.	User education, email filters, multi-factor authentication (MFA)
Ransomware	Malware encrypts files and demands ransom to restore access	Regular backups, endpoin protection, avoid suspicio downloads or links.
DDoS (Distributed Denial of Service)	Overwhelms servers with traffic, causing outages	Use firewalls, DDoS protection services, traffic filtering and rate limiting.
SQL injection	Injects malicious SQL code into web input fields to manipulate databases.	Use parameterized queri input validation and web application firewalls (WAFs
Man-in-the-middle (MitM)	Intercepts communication between two parties	Use end-to-end encryption (SSL/TLS), VPNs, secure Wi-fi.
Brute force Attack	Repeated attempts to guess passwords using trial and error.	Enforce strong password policies, account lockouts and CAPTCHA.
Zero-Day Exploit	Targets a vulnerability before it's publicly known or patched	Regular software updates, threat intelligence monitorin behaviour-based detection

Date: / /

Cyber Attack	Description	Mitigation Techniques
Cross-Site Scripting (XSS)	Injects malicious scripts into trusted websites.	Sanitize user inputs, use content security policy (CSP) and escape output data
Credential stuffing	Uses leaked username/ password combinations to gain access to accounts	Enable MFA, monitor for suspicious login behaviour and encourage password uniqueness,
Social Engineering	Manipulates people into revealing confidential information.	Security awareness training, verification protocols and simulated attack testing.

Caesar Cipher

A-Z alphabets are counted as 0-25 serially



Date : / /

Caesar Cipher:

One of the oldest and simplest substitution ciphers. Each letter in the plaintext is shifted by a fixed number(K) positions in the alphabet.

Formula used to encrypt and decrypt:

Encryption : $C = (P+K) \bmod 26$

Decryption : $P = (C-K) \bmod 26$

decrypt by subtracting

detailed description

For O, $(17-3) \bmod 26$

$= 14 \bmod 26 \rightarrow 26\overline{)14}(0$

$= 14$

if $26 \bmod 14 \rightarrow 14\overline{)26}(1$, $\frac{14}{12}$

answer

P = plaintext letter number

C = ciphertext letter number

K = key (shift value)

Example: P = Hello

K = 3

It is important to convert into numbers since when id=key will be given larger numbers would need the formula to be used.

encryption

1. Convert to numbers : H = 7, E = 4, L = 11, L = 11, O = 14
2. Add shift (K = 3): $H(\overset{P}{7}) + \overset{K}{3} = 10 \rightarrow K$

   $E(4) + 3 = 7 \rightarrow H$

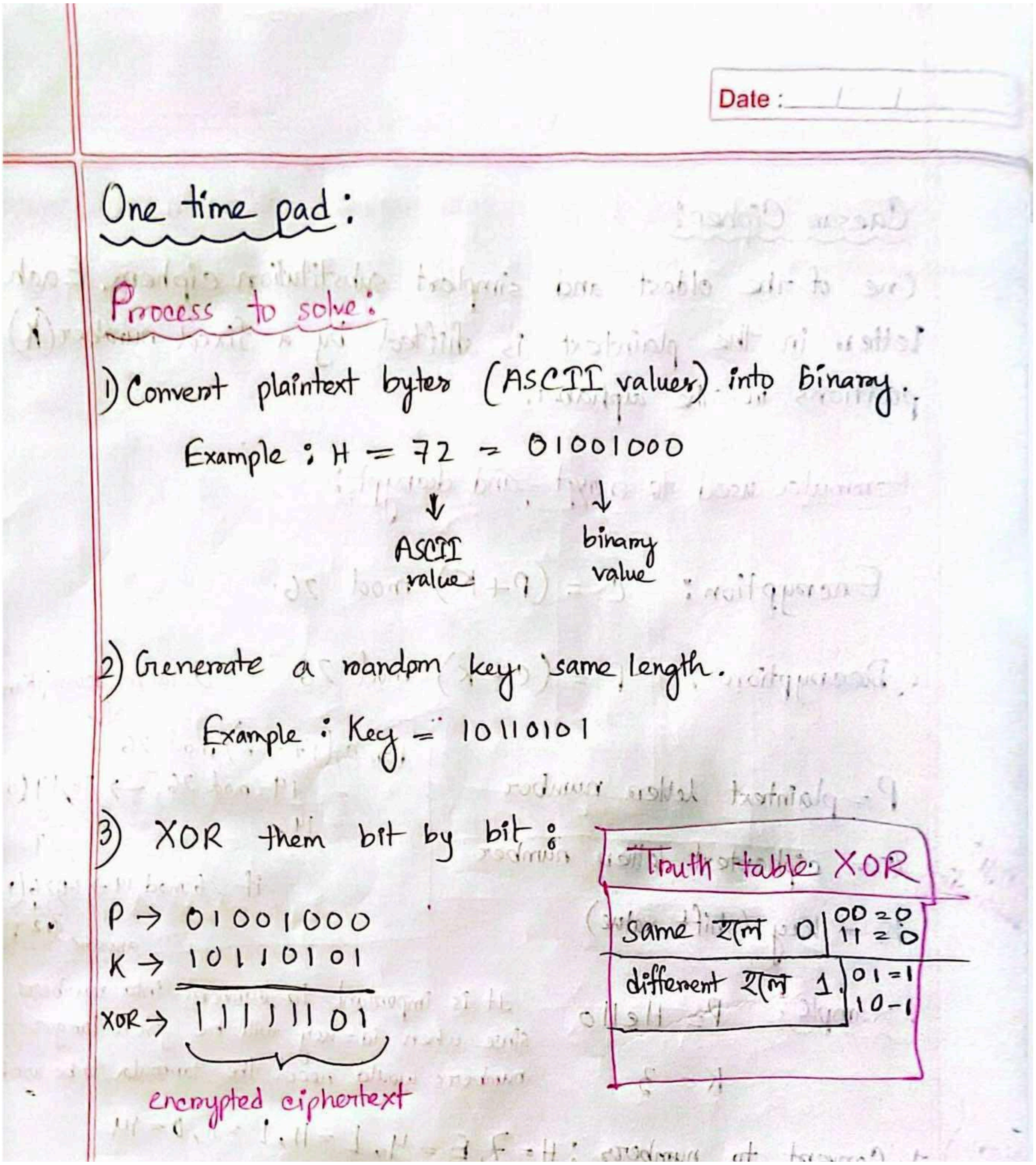
   $L(11) + 3 = 14 \rightarrow O$

   $L(11) + 3 = 14 \rightarrow O$

   $O(14) + 3 = 17 \rightarrow R$

   Use formula $(7+3) \bmod 26 = 10$
3. Ciphertext = KHOOR

One Time Pad



Date : / /

One time pad :

Process to solve :

1) Convert plaintext bytes (ASCII values) into binary.

Example : $H = \underset{\text{ASCII value}}{72} = \underset{\text{binary value}}{01001000}$

2) Generate a random key same length.

Example : Key = 10110101

3) XOR them bit by bit :

$$\begin{array}{ll} P \rightarrow & 01001000 \\ K \rightarrow & 10110101 \\ \hline XOR \rightarrow & \underbrace{11111101}_{\text{encrypted ciphertext}} \end{array}$$

Truth table XOR	
same হলে 0	00 = 0 11 = 0
different হলে 1.	01 = 1 10 - 1

Assignment sample

- Take a sentence
- Generate a key of same length
- Encrypt the sentence using the key with one time pad (ASCII value of whitespace is 20(hx))
- Decrypt the ciphertext and check if you get back the original text.

Example:

Plaintext: HELLO WORLD
Key: XWYXIHVZBNZ (uppercase letters, same length)
Ciphertext (in hexadecimal): [10,12,15,14,06,68,01,15,10,02,1e]
Decrypted Text: HELLO WORLD

ASCII VALUES

Space " " = 32

0–9 = 48 to 57

A-Z = 65-90

a-z = 97-122

There are several other ASCII values for certain symbols like: , . ! < >
Pray if these are given then their ASCII values will also be mentioned🙂

Encryption:

Plaintext: HELLO WORLD

Key: XWYXIHVZBNZ

Char	ASCII (dec)	Binary
H	72	01001000
E	69	01000101
L	76	01001100
L	76	01001100
O	79	01001111
(space)	32	00100000
W	87	01010111
O	79	01001111
R	82	01010010
L	76	01001100
D	68	01000100

Char	ASCII (dec)	Binary
X	88	01011000
W	87	01010111
Y	89	01011001
X	88	01011000
I	73	01001001
H	72	01001000
V	86	01010110
Z	90	01011010
B	66	01000010
N	78	01001110
Z	90	01011010

Now after configuring the **ASCII values** and **Binary values** from the **Plaintext and Key** The process to Encrypt the message is using XOR

Ciphertext, C = P⊕K

Example:

- H (72 = 01001000) **XOR** (88 = 01011000) = 18 (00010010)

In the same process calculating for all other letters:

Plain (dec)	Key (dec)	XOR result	Cipher (hex)
72 (H)	88 (X)	16	10h
69 (E)	87 (W)	18	12h
76 (L)	89 (Y)	21	15h
76 (L)	88 (X)	20	14h
79 (O)	73 (I)	6	06h
32 ( )	72 (H)	104	68h
87 (W)	86 (V)	1	01h
79 (O)	90 (Z)	21	15h
82 (R)	66 (B)	16	10h
76 (L)	78 (N)	2	02h
68 (D)	90 (Z)	30	1Eh

Ciphertext (in hexadecimal): [10,12,15,14,06,68,01,15,10,02,1e]

Decryption:

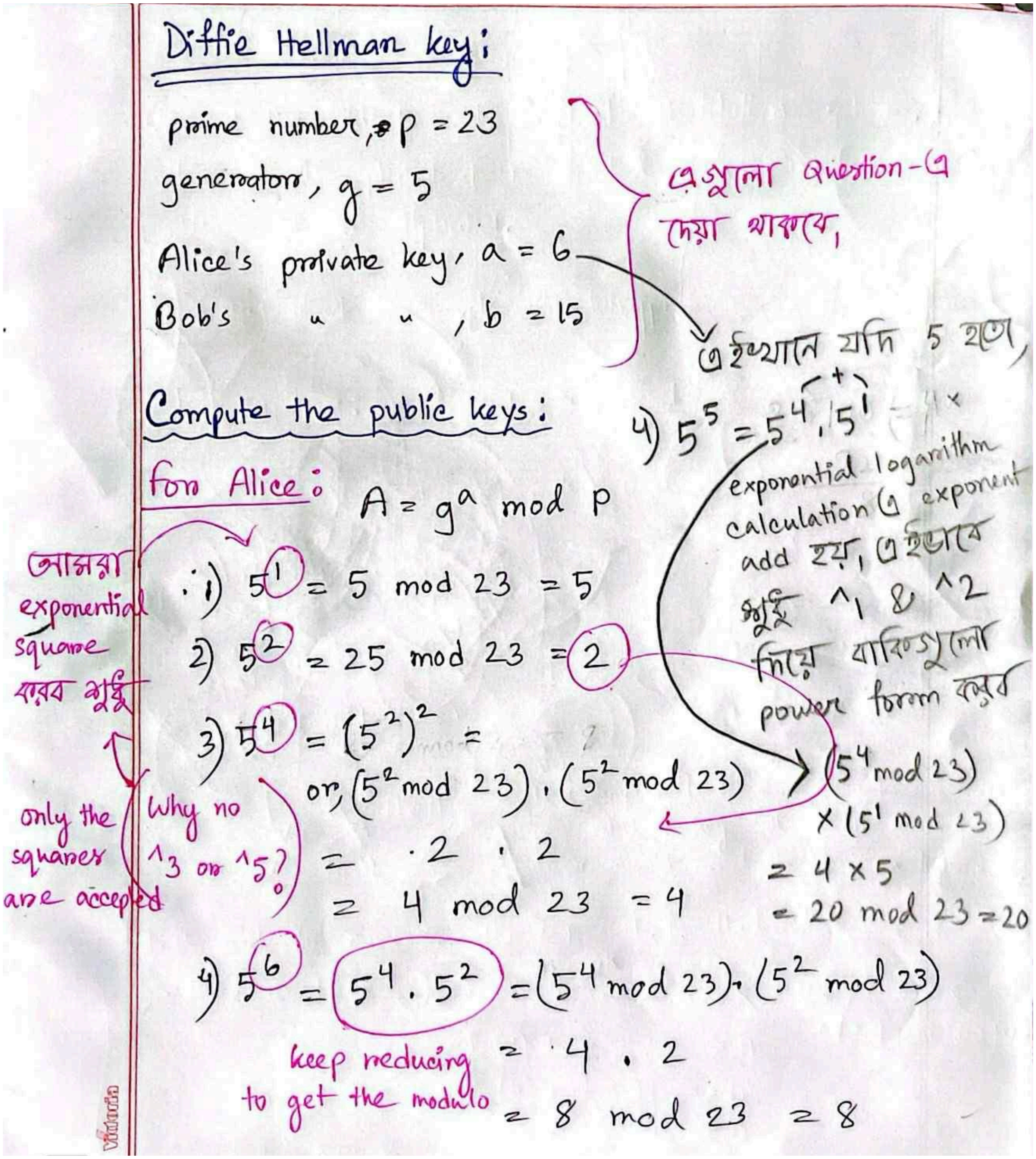
Decryption uses the same XOR:

$$\mathbf{P=C\oplus K}$$

If we XOR each ciphertext byte with its key byte → we get back original:
Plaintext, p = HELLO WORLD

Diffie Hellman Key

Diffie Hellman youtube video for better understanding



Diffie Hellman key:

prime number, $p = 23$

generator, $g = 5$

Alice's private key, $a = 6$

Bob's 〃 〃 , $b = 15$

এগুলো Question-এ দেয়া থাকবে,

এইখানে যদি 5 হতো,

4) $5^5 = 5^4 . 5^1$

exponential logarithm calculation এ exponent add হয়, এইভাবে শুধু ^1 & ^2 দিয়ে বাকিগুলো power form করব

$(5^4 \bmod 23)$
$\times (5^1 \bmod 23)$
$= 4 \times 5$
$= 20 \bmod 23 = 20$

Compute the public keys:

for Alice: $A = g^a \bmod p$

আমরা exponential square করব শুধু

only the squares are accepted

Why no ^3 or ^5?

1) $5^1 = 5 \bmod 23 = 5$

2) $5^2 = 25 \bmod 23 = 2$

3) $5^4 = (5^2)^2 =$
or, $(5^2 \bmod 23) . (5^2 \bmod 23)$
$= 2 . 2$
$= 4 \bmod 23 = 4$

4) $5^6 = 5^4 . 5^2 = (5^4 \bmod 23) . (5^2 \bmod 23)$
$= 4 . 2$
$= 8 \bmod 23 = 8$

keep reducing to get the modulo

Date : / /

for Bob :

$$B = g^b \bmod P$$

$$= \boxed{5^{15}} \bmod 23$$

$$23)\,5\,(\,0$$
$$\underline{0}$$
$$\boxed{5}$$

mod আসলে remainder নিবো

Breaking the 5^{15} stepwise:

1) 5^1 ~~mod~~ $= 5 \bmod 23 = 5$

2) $5^2 = 25 \bmod 23 = 2$

3) $5^4 = (5^2 \bmod 23) \times (5^2 \bmod 23)$

$= 2 \times 2 = 4 \bmod 23 = 4$

why 5^6 not taken?
↓
we can form 5^8 by $4+4$ from $5^4 . 5^4$

4) $5^8 = (5^4 \bmod 23) \times (5^4 \bmod 23)$

$= 4 \times 4 = 16 \bmod 23 = 16$

5) $\boxed{5^{15}} = 5^{8} \overset{+}{\frown} \times 5^{4} \overset{+}{\frown} \times 5^{2} \overset{+}{\frown} \times 5^{1}$.

$= 16 \times 4 \times 2 \times 5$ → reduced the previous mod answers of the power.

$= 640 \bmod 23$

$= \boxed{19}$. public key

Public keys:

Alice, A = 8

Bob, B = 19

Now, calculate the shared secret key:

$$\left.\begin{aligned} S &= B^a \bmod P \\ &= 19^6 \bmod 23 \end{aligned}\right\}$$ For Alice; they exchange their public keys to create a secret key.

$$\left.\begin{aligned} S &= A^b \bmod P \\ &= 8^{15} \bmod 23 \end{aligned}\right\}$$ For Bob

Alice :

1) $19^1 = 19 \bmod 23 = 19$

2) $19^2 = 361 \bmod 23 = 16$

3) $19^4 = 16^2$ $\left\{\begin{aligned} &(19^2 \bmod 23) \times (19^2 \bmod 23) \\ &= 16 \times 16 \\ &= 16^2 \end{aligned}\right\}$ বুঝায় লেখার জন্য বুঝা গেলে write short to save time!

final ~~key~~ step to discover secret key

$= 256 \bmod 23 = 3$

4) $19^6 = 19^4 \times 19^2 = 3 \times 16 = 48 \bmod 23$

$= \boxed{2}$ → secret key

Alice & Bob will find the same secret key →

Date : / /

Bob :

1) $8^1 = 8 \bmod 23 = 8$

2) $8^2 = 64 \bmod 23 = 18$

3) $8^4 = 18^2 = 324 \bmod 23 = 2$

4) $8^8 = (8^4 \times 8^4) = 4 \bmod 23 = 4$

5) $\boxed{8^{15}} = 8^8 \times 8^4 \times 8^2 \times 8^1$

$= 4 \times 2 \times 18 \times 8$

$= 1152 \bmod 23$

$= \boxed{2}$

$\therefore$ Both get the same secret key, $s = 2$

More math example with different values:

Step 0: Choose public numbers

- Prime number p=17 (small for simplicity)
- Generator g=3

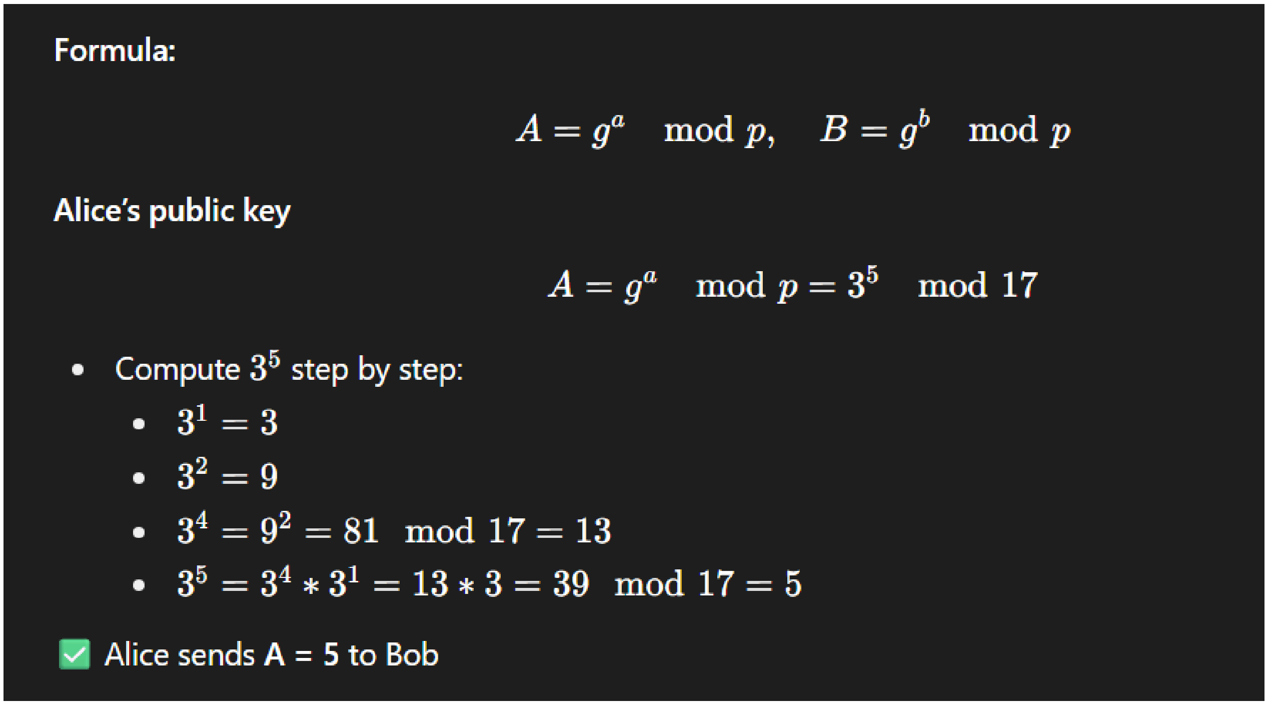
These are **public**, everyone can see them.

Step 1: Choose private keys

- Alice chooses a=5 (secret)
- Bob chooses b=7(secret)

Private keys are **never shared.**

Step 2 : Calculate the public keys



Formula:

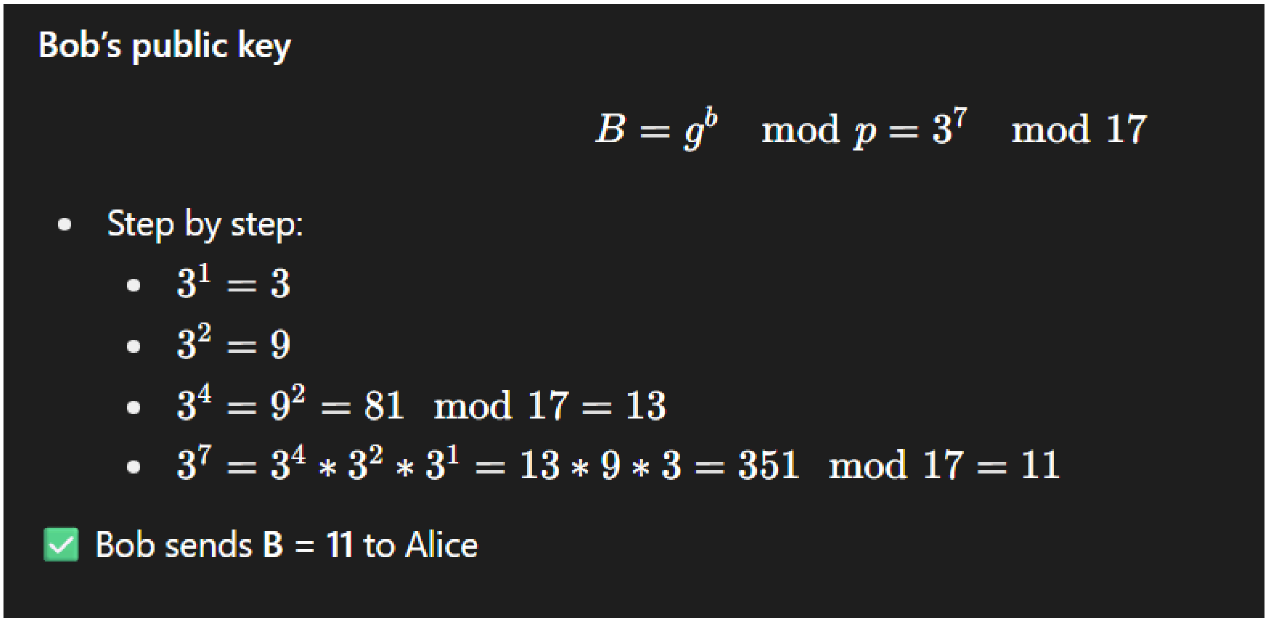
$$A = g^a \mod p, \quad B = g^b \mod p$$

Alice's public key

$$A = g^a \mod p = 3^5 \mod 17$$

- Compute 3^5 step by step:
  - $3^1 = 3$
  - $3^2 = 9$
  - $3^4 = 9^2 = 81 \mod 17 = 13$
  - $3^5 = 3^4 * 3^1 = 13 * 3 = 39 \mod 17 = 5$

✅ Alice sends A = 5 to Bob



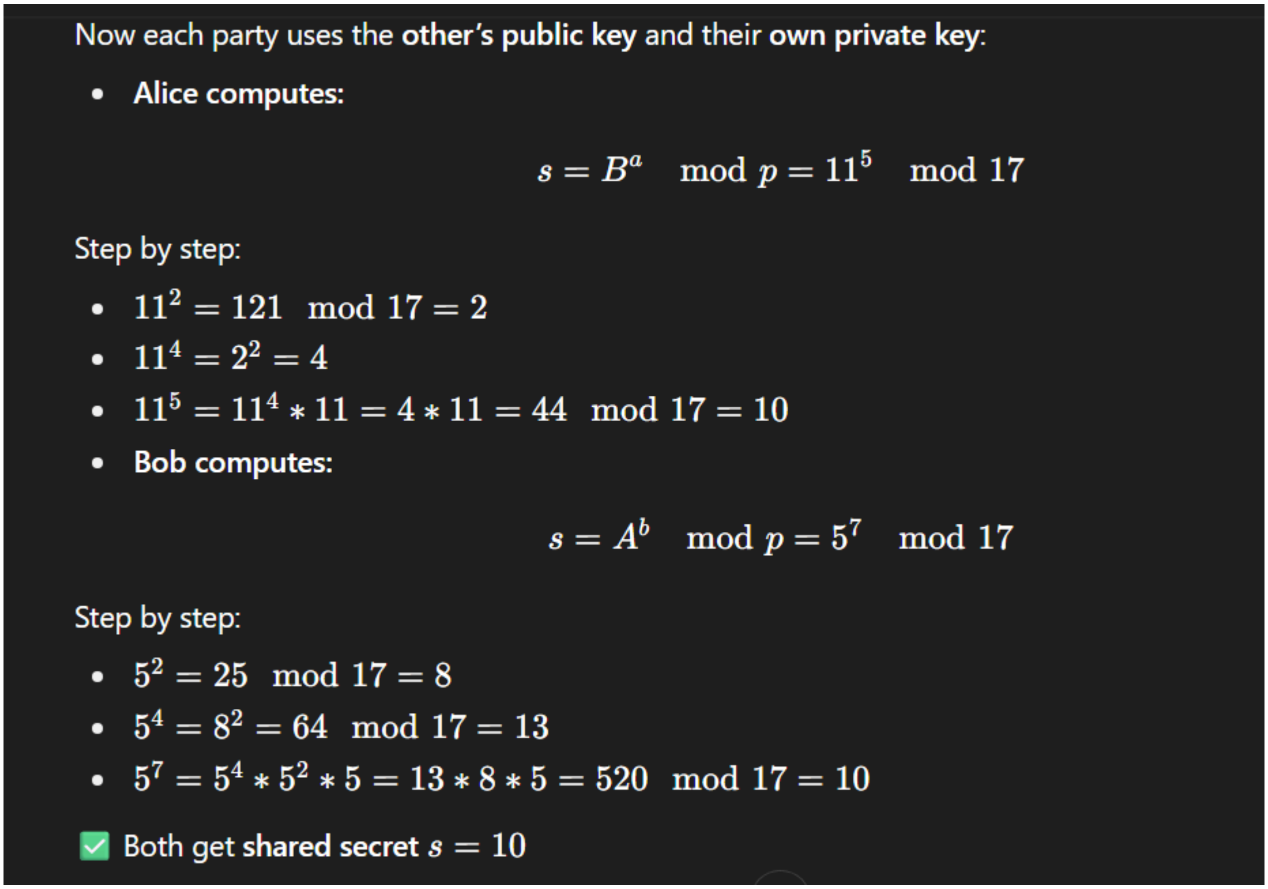
Bob's public key

$$B = g^b \mod p = 3^7 \mod 17$$

- Step by step:
  - $3^1 = 3$
  - $3^2 = 9$
  - $3^4 = 9^2 = 81 \mod 17 = 13$
  - $3^7 = 3^4 * 3^2 * 3^1 = 13 * 9 * 3 = 351 \mod 17 = 11$

✅ Bob sends **B** = 11 to Alice

Step 3 : Calculate the shared secret key



Now each party uses the **other's public key** and their **own private key**:

- **Alice computes:**

$$s = B^a \mod p = 11^5 \mod 17$$

Step by step:

- $11^2 = 121 \mod 17 = 2$
- $11^4 = 2^2 = 4$
- $11^5 = 11^4 * 11 = 4 * 11 = 44 \mod 17 = 10$
- **Bob computes:**

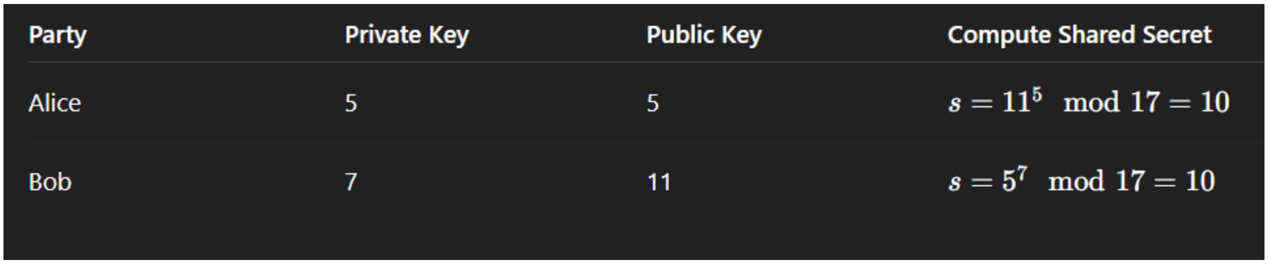
$$s = A^b \mod p = 5^7 \mod 17$$

Step by step:

- $5^2 = 25 \mod 17 = 8$
- $5^4 = 8^2 = 64 \mod 17 = 13$
- $5^7 = 5^4 * 5^2 * 5 = 13 * 8 * 5 = 520 \mod 17 = 10$

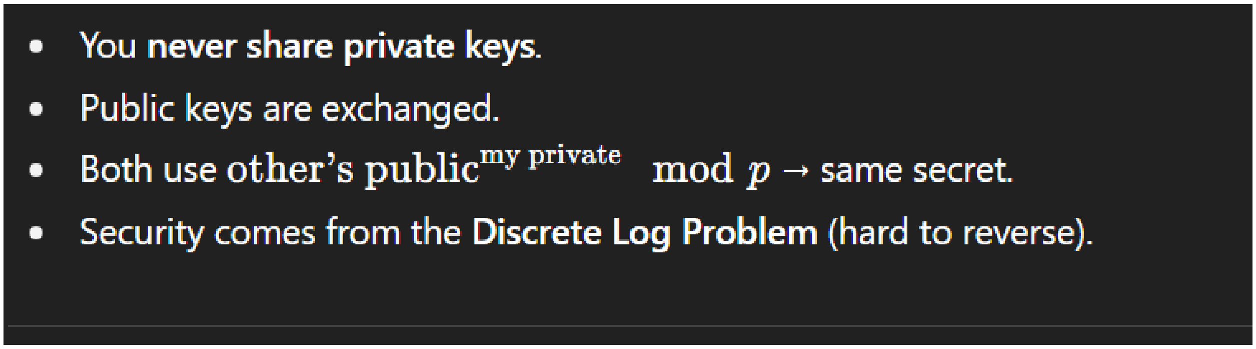
✅ Both get **shared secret** $s = 10$

Step 4: Summary table



Party	Private Key	Public Key	Compute Shared Secret
Alice	5	5	$s = 11^5 \mod 17 = 10$
Bob	7	11	$s = 5^7 \mod 17 = 10$

Key points to remember:



- You **never share private keys**.
- Public keys are exchanged.
- Both use $\text{other's public}^{\text{my private}} \mod p$ → same secret.
- Security comes from the **Discrete Log Problem** (hard to reverse).

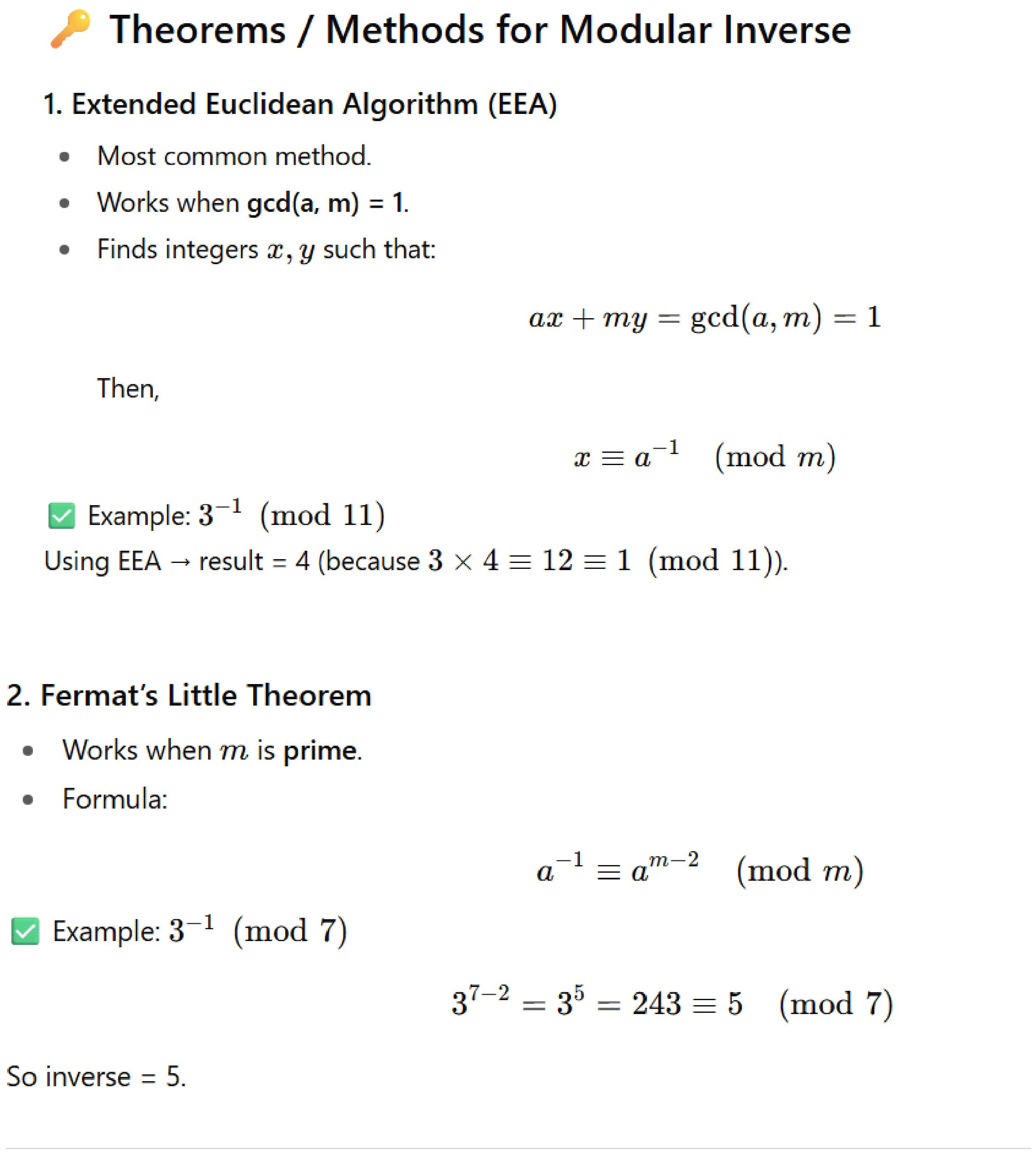
(AES)Advanced Encryption Standard

AES: How to Design Secure Encryption

Eita janina ki porbo keu janle inbox koro

Modular Inverse

Nije korle handwritten notes add kore dibo….



🔑 Theorems / Methods for Modular Inverse

1. Extended Euclidean Algorithm (EEA)

- Most common method.
- Works when **gcd(a, m)** = 1.
- Finds integers x, y such that:

$$ax + my = \gcd(a, m) = 1$$

Then,

$$x \equiv a^{-1} \pmod{m}$$

✅ Example: $3^{-1} \pmod{11}$

Using EEA → result = 4 (because $3 \times 4 \equiv 12 \equiv 1 \pmod{11}$).

2. Fermat's Little Theorem

- Works when m is **prime**.
- Formula:

$$a^{-1} \equiv a^{m-2} \pmod{m}$$

✅ Example: $3^{-1} \pmod{7}$

$$3^{7-2} = 3^5 = 243 \equiv 5 \pmod{7}$$

So inverse = 5.

3. Euler's Theorem

- More general than Fermat's (works when $\gcd(a, m) = 1$, not just prime m).
- Formula:

  $$a^{\varphi(m)} \equiv 1 \pmod{m}$$

  So,

  $$a^{-1} \equiv a^{\varphi(m)-1} \pmod{m}$$

  (where $\varphi(m)$ = Euler's totient function).

✅ Example: $3^{-1} \pmod{10}$
$\varphi(10) = 4$.

$$3^{\varphi(10)-1} = 3^3 = 27 \equiv 7 \pmod{10}$$

So inverse = 7.

Difference between Symmetric and Asymmetric Key Cryptography

Feature	Symmetric Key Cryptography	Asymmetric Key Cryptography
Number of keys	1 key (same for encryption & decryption)	2 keys (Public & Private pair)
Key relation	Same key is shared	Keys are mathematically related
Speed	Very fast	Slower (more computation)
Security	Key distribution is a problem	More secure for sharing keys
Use cases	Encrypting large amounts of data (e.g., AES, DES)	Secure key exchange, digital signatures (RSA, DH, ECC)
Example analogy	One house key for both people	Mailbox (public address + private key to open)

Difference between public and private key

Aspect	Public Key	Private Key
Who holds it?	Shared with everyone	Kept secret by the owner
Function	Used to encrypt or verify	Used to decrypt or sign
Security	Safe to distribute	Must never be shared
Analogy	Your home address (anyone can send mail)	Your mailbox key (only you can open)