# CNS Assignment 1

Nikil. Lalwani D15B/37

Q1) Explain the difference between substitution cipher and transposition cipher.

| | Substitution Cipher | Transposition Cipher |
|---|---|---|
| 1) | In substitution cipher, plain text is substituted with numbers, alphabets and symbols. | In transposition cipher, plain text characters are rearranged with respect to position. |
| 2) | Two types : monoalphabetic substitution cipher and polyalphabetic substitution cipher. | Two types: keyed transposition cipher and keyless transposition cipher. |
| 3) | Character's identity is changed but position is same. | Characters position is changed but identity remains same. |
| 4) | Letter with low frequency can detect plaintext. | Keyes nearer to plaintext can disclose plain text. |
| 5) | Ceaser cipher is substitution cipher | Rail fence cipher is transposition cipher. |

Q2) Explain the difference in steganography and cryptography.

| | Steganography | Cryptography |
|---|---|---|
| 1) | Information is hidden in steganography. | Information is transformed in cryptography. |
| 2) | Hidden information is not visible. | Transformed information is visible. |
| 3) | Provides confidentiality only. | Provides confidentiality, integrity, non-repudiation. |
| 4) | No specific algorithm. | Various recognized and approved algorithm. |

Q3) Decipher the following cipher text using brute force attack:- "CMYMTOOEOORW".

Algorithm - Rail Fence

Key = 2

| C | | M | | T | | M | | T | | O | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | O | | E | | O | | O | | R | | W |

plain text - COME TOMOTROW

Q4) Encrypt the following using playfair cipher using the keyword - "MONARCHY" - "SWARAJ IS MY BIRTH RIGHT". Use X for blank space.

Key - MONARCHY

plaintext - SWARAJ IS MY BIRTH RIGHT.

Matrix -

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

SW AR AJ XI SM YX BI RT HX RI GH TX

QX RM BS AS LA BW IS DZ BV AK FY SZ

Cipher text - QXRMBSASLABWISDZBVAKFYSZ.

Q5) Apply Caesar cipher k=5 and decrypt the given cipher text - "YMJJYMJWXNIJJKXNQJSHJ".

For encryption -

$$C = (P + K) \% 26$$

For decryption -

$$D = (P - K) \% 26$$

| Y | M | J | T | Y | M | J | W | X | N | I | J | T | K | X | N | P | J | S | H | J |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 24 | 12 | 9 | 19 | 24 | 12 | 9 | 22 | 23 | 13 | 8 | 9 | 19 | 10 | 23 | 13 | 16 | 9 | 18 | 7 | 9 |
| 19 | 7 | 4 | 14 | 19 | 7 | 4 | 17 | 18 | 8 | 3 | 4 | 14 | 5 | 18 | 8 | 11 | 4 | 13 | 2 | 4 |
| T | H | E | O | T | H | E | R | S | I | D | E | O | F | S | I | L | E | N | C | E |

Plaintext after decryption-
"The other side of silence."

Q6) Apply vigenere cipher, encrypt "explanation" using key "leg".

key - leg
plaintext - explanation.

| l | e | g | l | e | g | l | e | g | l | e |
|---|---|---|---|---|---|---|---|---|---|---|
| e | x | p | l | a | n | a | t | i | o | n |
| 7 | 19 | 9 | 0 | 4 | 7 | 11 | 15 | 2 | 3 | 9 |
| H | t | j | a | e | h | l | p | c | d | j |

cipher text - htjaehlpcdj

Q7) Compare symmetric and asymmetric cryptography.

| | Symmetric | Asymmetric. |
|---|---|---|
| 1) | Same key for encryption & decryption. | Using a pair of key: public key, private key for encryption & decryption. |
| 2) | Simple as only one key is used. | More complex as two keys are used. |
| 3) | Faster execution speed. | Comparatively slower. |
| 4) | AES, DES are common algorithm. | RSA & Diffie-Hellman are common algorithm. |

Q8) Explain AES along with its major attributes.

Ans i) AES stands for Advanced Encryption Standard.

ii) DES was replaced by AES.

iii) It is symmetric key based algorithm.

iv) Works as a block cipher

v) It uses 128-bit key.

vi) It can work with 128, 192 & 256 bit key

vii) No. of rounds of operation depends upon key size
128 bit key 10 rounds
192 bit key 12 rounds
256 bit key 14 rounds.

viii) AES is considered highly secure due its long key sizes and is used in industry today.

9a) Explain different block cipher modes of operation.

| Mode | Description | Application. |
|---|---|---|
| 1) Electronic Code Book (ECB) | Each block of plaintext bits is encoded independently using the key. | Secure transmission of single value. |
| 2) Cipher Block chaining (CBC) | The input to encryption algorithm is XOR of the next block of plaintext and preceding block of ciphertext. | Authentication.<br>General purpose block oriented transmission. |
| 3) Cipher feedback (CFB) | Input is processed s bits at a time. Preceding ciphertext is used as input to the encryption algorithm to produce pseudorandom output which is XORed with plaintext to produce | Authentication<br>General purpose stream-oriented transmission. |

| | | |
|---|---|---|
| | next unit of ciphertext. | |
| 4) Output Feedback (OFB) | Similar to CFB, except that the input to the encryption algorithm is the preceding encryption output and full blocks are used. | Stream-oriented transmission over noisy channels (eg satellite communication) |
| 5) Counter (CTR) | Each block of plaintext is XORed with an encrypted counter. The output is incremented for each subsequent block. | General purpose block oriented transmission. Useful for high speed requirements |

Q10) Explain rootkits and its types.

Ans a) Rootkits are malicious software that give hackers full access to your PC.

b) It helps hackers to change or alter the system settings or files the way an administrator could do.

c) Rootkit is derived from two words - 'root' and 'kit'. Root is full access user account in Unix and kit represents a collection of tools.

d) Types of rootkits -

i) Hardware or firmware rootkit -
Rootkit is installed on your hardware. can affect PC's hard disk or BIOS.

Hackers can use this to intercept data written on hard drive.

ii) Bootloader rootkit-
Bootloader loads computer's OS.
This rootkit attacks and replaces legitimate bootloader.
This means the rootkit is active even before the OS.

iii) Memory rootkit-
Hides in RAM or Random Access Memory.
Carries out harmful activity in background.
But only live till the computer is rebooted.

iv) Application rootkit-
Replace standard files with rootkit files.
Affects programs such as word, paint etc.
Run every time a affected program is running.
Difficult to detect, as affected program run normally.

v) Kernel mode rootkits:-
Target core of PC's OS.
This can give easy access to computer and steal your information.

Q11) Explain DDos attack.
Ans a) DDOS stands for distributed denial of service.
This involves sending large amount of traffic to a website from multiple sources to overwhelm it.

b) In this malicious network attack, hackers send traffic from multiple network connected devices for communication to one website to overwhelm it with false traffic or requests.

c) This helps to ~~type~~ tie up all resources for request and crash or distract it so normal users cannot acuss it.

d) This attacks consist of multiple affected device called as bots and a group is called botnet.

e) Once a botnet is established, attacker is able to send remote instructions.

f) All bots then send request to website's IP address causing DDOS.

g) As all bots are legitimate devices, separating them from normal traffic is difficult.

q12) Explain various measures against social engineering attacks from individual user perspective and organizational perspective.

Ans a) Best defence is to be watchful.

b) As an individual-

Don't open emails from strangers

Don't provide important info such as cvv, date of birth to others.

Do not click on every ~~email~~ link you get.

c) As an organisation -

Provide training to all employees
Have corporate cybersecurity program for adequate digital security.
Setup an internal team for employee's to communicate to.