Name : Tejas Redkar
Roll NO : PC-44
Panel-C, Batch-C2
PRN: 1032210937

A+ Ug
30/11/23

ICS Lab Assignment - 1

* FAQ's

Q1) What are various classical ciphers?

Ans Classical ciphers are historical encryption techniques that were used to secure the confidentiality of messages before the advent of modern cryptography. These ciphers oftenrely ~~really~~ on simple mathematical pricinciples & ~~substitutions~~ substitutions. Here are some of the most well-known classical ciphers:

1) Caesar Ciphers: Named after Julius Caesar, this is one of the simplest substitution ciphers. It involves shifting each letter in the plaintext by a fixed number of positions down our up the alphabet. The shift value is called the "key".

2) Substitution ciphers: In this type of cipher, each letter in the plaintext is replaced with another letter based on a predetermined key. The most famous example is the Atbash cipher, where each

letter is replaced by its reverse in the alphabet.

3) Vigenere Cipher: Named after Blaise de Vigenere, this is a polyalphabetic substitution cipher. Instead of using a single shift value for the entire message, it uses a keyword to determine different shift value for different parts of the message.

4) Playfair Cipher: Invented by Charles Wheatstone but popularized by lord Playfair, this cipher uses a 5×5 grid of letters to encrypt pairs of letters in plaintext. It is a diagraph substitution cipher.

5) Transposition Cipher: Unlike substitution ciphers, transposition ciphers do not replace letters. Instead, they rearrange the order of letter in the plaintext.

Q2) Compare Steganography & Cryptography.

Ans Steganography & cryptography are two distinct techniques used to secure information, but they serve different purposes & employ different methods. Here's a comparision of the two:

① Purpose:

CRYPTOGRAPHY: The primary purpose of cryptography is to protect the confidentiality & integrity of information. It involves encoding plaintext into ciphertext using various algorithms & keys to prevent unauthorized access or tampering.

STEGANOGRAPHY: Steganography aims to conceal the existence of information within other data in such a way that the hidden information is difficult to detect.

② Concealment vs transformation:

CRYPTOGRAPHY: ~~Cryptography~~ Cryptographic techniques transform the original data (plaintext) into an unintelligible form (ciphertext) using algorithms & keys. The original data becomes obscure.

STEGANOGRAPHY: Steganographic techniques hide data within other data by subtly altering the carrier data without significantly changing its appearances.

③ Detection

CRYPTOGRAPHY: Cryptoanalysis is the process of attempting to decipher encrypted messages without

the correct key. If the encryption algorithm & key are strong.

STEGANOGRAPHY: Detecting hidden data in steganographic content is challenging & relies on statistical analysis, pattern recognition or specialized tools.

Q3) State the reasons why classical ciphers are obsolete?

Ans Classical ciphers, while historically significant, are considered obsolete in modern cryptography for several reasons.

1) Lack of Security: Classical ciphers are relatively simple & can be easily broken with modern computing power & cryptographic analysis techniques.
2) Limited key space: Classical ciphers often have a limited key space, making them susceptible to brute-force attacks.
3) Single-~~key~~ use keys: Many classical ciphers, especially the ones used historically, relied on single-use keys, making them vulnerable to compromise if the key was ~~interrupted~~ intercepted or revealed.
4) No Forward secrecy: Classical ciphers lack forward secrecy, meaning that if any adversary captures a message encrypted with

the same key if they obtain it later.

5) No authentication : Classical ciphers typically do not provide any means of messages authentication.

Q4) How to carry over cryptoanalysis of classical cryptography.

Ans Cryptoanalysis of classical cryptography involves the process of analyzing & breaking classical encryption technique such as substitution cipher, transposition cipher & other early cryptographic methods.

(1) Gather information : Collect as much information as possible about ciphertext, including frequency of characters, known patterns & any other clues about the encryption.

(2) Determine the type of cipher : Identify the type of classical cipher used - Substitution cipher
- Transposition cipher
- Viegnére Cipher
- Playfair cipher.

(3) Frequent Analysis : For substitution cipher, performs frequency analysis on the ciphertext. Count the frequency of each letter or symbol in the ciphertext.

(4) Trial & Error : If you suspect a substitution

cipher, start with basic technique like the caesar cipher & try decrypting the message.

(5) Pattern Recognition: look for pattern & repetition in the cipher text.

(6) Known-plaintext attack: You can use this information to deduce the key or encryption method.

(7) Brute Force attack: Attempt brute force attack by trying all possible key or key combinations.

(8) Expertise & tools can automate many of the above steps.

(9) Persistence: Cryptanalysis can be challenging & time consuming.

(10) Document your work.

Q5) Write how different disciplines of art, science & ~~English~~ engineering have contributed for information security.

Ans Information security is a multidisciplinary field that derives on various disciplines, including art, sciences & engineering, to develop strategies & technologies to protect data &

the message.

information systems.

① Art: User Experience (UX) Design: Good UX design ensures that security measures are easy for users to understand.

Science :- ① Cryptography: Science of encoding & deciving information to protect it from unauthorized access.

② Forensics

③ Engineering - Secure Systems Design
- Network security
- Physical security

④ Interdisciplinary Collaborations
- Ethical Hacking
- Human factores
- Legal & compliance
- Risk Management.

30/11/23