Amit Agrawal (10321f0293)

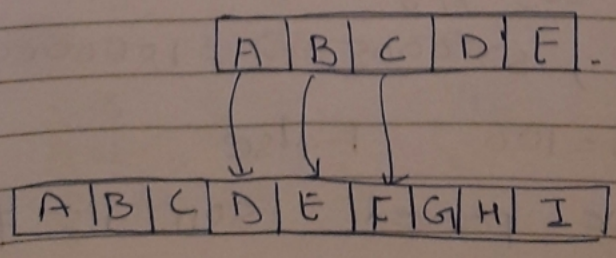
IS

DATE

Lab A1: Implement any classical cryptograp technique using Java or python c++

Theory: Caesar Cipher in Classical Cryptog

* The Caesar cipher technique is one of the earliest & simplest method of encryption technique. It's simply a type of substitution cipher i.e. each letter of of a given text is replaced by a letter some fixed number of positions down the alphabet. For example with a shift of 1, A would be replaced by B, B would become C & so on. The method is named after Julius Ceasar, who apparentl used it to communicate with his officials. Thus to cipher a given text we need a integer value, known as shift which indicates the number of position each let of the text has been moved down. The encryption can be represented using modular arithmetic by first transforming the letters into numbers



Encryption Phase with shift 3

classmate

PAGE

DATE

Algorithm for ceasar cipher
Input:
1. A string of lower case letters called text
2. An Integer between 0-25 denoting required shift

Procedure
- Traverse the given text one character at a time.
- For each character, transform the given character as per rule, depending on wether we're encrypting or decrypting the text
- Return the new string generated.

* Monoalphabetic substitution
In cryptography, a substitution cipher is a method of encoding by which units of plaintext are replaced with ciphertext according to a regular system; the units may be single letters, pairs of letters triplets of letters, mixture of above & so forth. The reciver deciphers the text by performing an inverse substitution.
A monoalphabetic cipher uses fixed substitution over the entire message whereas polyalphabetic cipher uses a number of substitutions at different position in the message, where a unit form the plaintext is mapped to one

DATE

one of several possibilities in the ciphertext & vice versa.

Conclusion : Thus we studied basic classical cryptographic, which are symmetric in nature & were used in the past. Mostly classical system are outdated, but important to understand

FAQ's

1. What are various classical ciphers?
→ classical cipher is a type of cipher that was used in past but for most part, has fallen into disuse.
The two main types of classical ciphers are
a) Substitution Cipher
In a substitution cipher, letter's are replaced throughout the text by another letter. The famoust substitution cipher are monoalphabetic substitution cipher & polyalphabetic substitution cipher

b) Transposition Cipher
In transposition cipher, the letters themselves are kept unchanged, but their order within the message is

DATE

scrambled according to some logic.

2. Compare steganography & Cryptography.

→

Steganography	Cryptography
1. Stegnography means covered writing	1. Cryptography means secret writing
2. Attacks are called steganalysis	2. Attacks are called cryptanalysis
3. Structure of data is not usally altered	3. Structure of data is altered
4. Not much of mathematical transformation is performed	4. Mathematical transformation is performed
5. The fact that secret communication is taking place is hidden	5. Only secret message is hidden.

3. State the reasons why classical ciphers are obsolete

→ The classical ciphers use same keys for encryption of plaint text & decryption of cipher with today's power of computation it's very easy to brute force attack to decrypt a cipher, Hence classical ciphers are obsolete.

PAGE

classmate

DATE

4. How to carry out cryptanalysis of classical cryptography

→ For classical cryptography, there is great possibility of brute force attack as we can test all possible keys as keys for encryption & decryption are same.

5. Write how different disciplines of art science & engineering have contributed for information security.

→ The early idea of cryptography which is used in information security heavily emerges from steganography. The steganography is a method of covered writing to communicate something confidential. Earlier it was considered as a art form but very few knew that it is being used for communicatio As science & technology advanced in late 19th century heavy used of mathematical transformation was starte to encrypt & decrypt text message & with use of high computation power the messages are encrypted & decrypted which makes it quite difficult for attacker to have access to those messages.

classmate

PAGE