Extracted Content (Slide 3)

Page 2 – Cryptography

- Cryptography: is the art of achieving security by encoding messages to make them non-readable.

Page 3 – Cryptanalysis

- Cryptanalysis: is the technique of decoding messages from a non-readable format back to
- Readable format without knowing how they were initially converted.
- To Identifying weaknesses of the algorithm.

Page 4 – Plain text and cipher text

- The message in the plain text can be understood by anybody knowing the language.
- For example: If we speak with our family members, friends or colleagues, we use plain text because we do not to hide anything from them.

Page 5 – Plain text and cipher text

- Definition: Clear text or Plain text signifies a message that can be understood by the sender, the receiver and also by anyone else who gets an access to that message.
- However, there are situations, where we are concerned about the secrecy of our conversations.
- Suppose the email is confidential for some reason.
- Usually the simplest trick that we use is a code language.

Page 6 – Cipher text

- One simple method of code language is that we replace each alphabet in our conversation with another one.
- The codified message is called Cipher text.

- Definition: When a plain text message is codified using any suitable scheme, the resulting message is called Cipher text.

Page 7 – Attacks Against Encryption

- Encryption systems can be attacked in three ways
- Through weaknesses in the algorithm
- Through brute force against the key
- Through weaknesses in the surrounding system.

Page 8 – Encryption

- There are two primary types of encryption:
  - Symmetric key Cryptography
  - Asymmetric key Cryptography
- Symmetric key Cryptography/Private key encryption requires all parties who are authorized to read the information to have the same key.
- Both the sender and the receiver of the information must have the same key.

Page 9 – Encryption Techniques

- Cryptography
- Symmetric Key Cryptography
- Classical Cryptography
- Substitutions Cypher
- Transpositions Cypher
- Modern Cryptography
- Stream Cypher
- Block Cypher
- Asymmetric Key Cryptography

Page 10 – Encryption Techniques

- There are two primary ways in which a plain text message can be codified to obtain the corresponding Cipher text:

1. Substitution
2. Transposition.

- Note: When the two approaches are used together, we call the technique as Product Cipher.

Page 11 – Substitution techniques (Caesar Cipher)

- The scheme explained earlier (replacing an alphabet with the one three place down) was first proposed by Julius Caesar and is termed as Caesar Cipher.
- Definition: In Substitution Cipher Technique, the characters of a plain text message are replaced by other characters, numbers or symbols.
- Caesar Cipher is a very weak scheme,
- To beak the Caesar cipher reverse the Caesar cipher process.

Page 12 – Algorithm to break Caesar cipher

1. Read each alphabet in the Cipher text message, and search for it in the second row of the replacement table.
2. When a match is found, replace that alphabet in the cipher text message with the corresponding alphabet in cipher text.
3. Repeat the process for all alphabets in the Cipher text message.

Page 13 – Modified version of Caesar cipher

- May not necessarily be three place down, but instead, it can be any place down.
- Thus, now an alphabet A in plain text would be replaced by any valid alphabet.
- Once the replacement scheme is decided, it would be constant and will be used for all other alphabets in that message.
- As we know, the English language contain 26 alphabets.
- Thus, an alphabet A can be any other alphabet in the English alphabet set, we have 25 possibilities of replacement.

Page 14 – Modified version of Caesar cipher

- An algorithm to break the modified caesar cipher.

1. Let K = 1;
2. Read the complete cipher text message.
3. Replace each alphabet in the cipher text message with an alphabet that is k positions down the order.
4. Increment k by 1

5. If K is less than 26, then go to step 2, otherwise stop the process.
6. It will be one of the 25 possibilities produced by the above steps.

Page 15 – Modified version of Caesar cipher

- Meet me after the toga party
- Phhw ph diwhu wkh wrjd sduwb
- An attack on a cipher text message, in which the attacker use all possible combinations,
- is called Brute-Force attack.

Page 16 – Modified version of Caesar cipher

- Three important characteristics of this problem enabled us to use a brute-force cryptanalysis:

1. The encryption and decryption algorithms are known.
2. There are only 25 keys to try.
3. The language of the plaintext is known and easily recognizable.

Page 17 – Activity

- Download and Install CrypTool.
- Use Some Random text as Plaint text/input and encrypt using Caesar cipher.
- Use Caesar cipher to Decrypt the cipher text back to plain text.

Page 19 – Mono-Alphabetic Cipher

- The weakness of the Caesar Cipher is that only 25 possible keys are required to break.
- A Permutation of a finite set of elements S is an ordered sequence of all the elements of S, in which each element appearing exactly once.
- For example, if S = {a, b, c}, there are six permutations of S:
  abc, acb, bac, bca, cab, cba
- In general, there are n! permutations of a set of n elements.

Page 20 – Mono-Alphabetic Cipher

- In the Caesar cipher, we replace each alphabet with the third alphabet,
- Instead, the “cipher” line can be any permutation of the 26 alphabetic characters
- Then there are 26! or greater than 4 x 10^{26} possible keys.
- This means that in a given plain text message, each A can be replaced by any other alphabet (B through Z), each B can be replaced by any other random alphabet (A or C through Z) and so on.
- This is extremely hard to crack.

Page 21 – Mono-Alphabetic Cipher

- A mono-alphabetic substitution cipher or simple substitution techniques or Atbash uses:
- Fixed substitution over the entire message.
- Such an approach is referred to as a mono-alphabetic substitution cipher.
- Because a single cipher alphabet (mapping from plain alphabet to cipher alphabet) is used per message.

Page 22 – Mono-Alphabetic Cipher

- There is only one hitch. If the cipher text created with this technique is short, the cryptanalyst can try different attacks based on her knowledge of the English language.

Page 23 – Homo-Phonic Substitution Cipher

- The Homo-Phonic Substitution Ciphers is very similar to Mono-alphabetic Cipher.
- We replace one alphabet with another in this scheme.
- However, the difference between the two techniques is that:
- The replacement alphabet set in case of the simple substitution techniques is fixed.
- In Homophonic Substitution Cipher, one plain text alphabet can map to more than one cipher text alphabet.

Page 24 – Homo-Phonic Substitution Cipher

- The letter e could be assigned a number of different cipher symbols, such as 16, 74, 35, and 21.
- With each homophone assigned to a letter in rotation or randomly.

Page 26 – Polygram Substitution Cipher

- In Polygram Substitution Cipher techniques, a block of alphabets is replaced with another block.
- The replacement of plain text happens block-by-block, rather than character-by-character.

Page 28 – Vigenère Cipher

- One of the simplest, Poly-alphabetic/Polygram Ciphers is the Vigenère cipher.
- This cipher uses multiple one-character keys.
- Each of the keys encrypts one plain text character.

Page 29 – Vigenère Cipher

- After all the keys are used, they are recycled.
- Every character would be replaced with the same key after repetition.

Page 30 – Vigenère Cipher

- The corresponding Cipher text letter is at the intersection of row titled key and column titled plain text.

Page 32 – Playfair Cipher

- It is also called Palyfair Square, is used for manual encryption of data.
- It is multiple-letter encryption cipher.
- The Playfair encryption scheme uses two main processes:

1. Creation and population of Matrix
2. Encryption Process

Page 33 – Playfair Cipher

- The Playfair algorithm is based on the use of a 5 x 5 matrix of letters constructed using a keyword.

Page 35–36 – Playfair Cipher

- Plain text is broken into groups of two alphabets.
- Same row → replace with right letter
- Same column → replace with below letter
- Otherwise → rectangle rule

Page 39–41 – Hill Cipher

- Hill cipher is Multi-letter Cipher.
- Letters are converted into numbers (A=0, B=1 … Z=25).
- Plain text is converted into matrix.
- Multiply with key matrix.
- Apply mod 26.
- Convert back to alphabets.

Page 46 – Transposition Techniques

- Involves permutation of plaintext letters instead of substitution.

Page 47 – Rail Fence Technique

- Plaintext is written diagonally and read row by row.

Page 48–49 – Columnar Transposition

- Plain text is written in rows and read in column order.

Page 51–53 – Multiple Transposition

- Same process is repeated multiple times to increase complexity.