Cryptography Types of ciphers

- *DigitalSherlock.com | SafeHack.com*
- *Date: 2005/05/27*
- *Document Name: cryptography_types_of_ciphers.pdf*
- *GNU Free Documentation License*
- *Version 1.00, 2005-05-27*
-

❖ Classical substitution ciphers

- **Replaces bits, characters, or blocks of characters with different bits, characters or blocks**
- **Replace one character with another**
- **Monoalphabetic substutution cipher**
  - **The same plaintext character is always encrypted to the same ciphertext character**
  - **Caesar cipher**
  - **Attack: frequency Analysis**
- **Polyalphabetic substitution cipher**
  - **Multiple possible ciphertext characters that may result from the encryption of the same plaintext character**
  - **Attack: frequency Analysis**

❖ Transposition (permutation) ciphers

- **Permutation is used, meaning that letters are scrambled**
- **The key determines the positions that the characters are moved to.**
- **Write the message vertically and read horizontally**
- **Plaintext remains the same, but the order of characters is shuffled around**
- **Can be attacked through frequency analysis**

❖ Polyalphabetic Ciphers

- **Also known as Vigenere Cipher**
- **Caesar is a subset of the Vigenere Polyalphabetic Cipher**
- **Vigenere used 26 alphabets**
- **Each letter of the message corresponds to a different alphabet**
- **Uses different alphabets to defeat frequency analysis**
- **The key is not repeated**
- **Subject to guessing the period, when the alphabet changes**

❖ Block Cipher

- **Operate on fixed size blocks of plain text**
- **Breaks the plaintext into blocks and encrypts each with the same algorithm**
- **Apply an identical encryption algorithm and key to each block**
- **The properties of a cipher should contain confusion and diffusion**
- **Diffusion**
  - **Spread the plaintext character over many ciphertext characters. Done using permutations**

- **Different unknown key values cause confusion**
- **Putting the bits within the plaintext through many functions cause diffusion**
- **N Accomplished through p-boxes**
- **DES implements this product 16 times**

➢ **Confusion**

- **Conceals statistical connection using substitution**
- **N Accomplished through s-boxes**
- **Block cipher use S-boes**
- **An S-box is non-linear because it generates a 4-bits output string from 6 bits input**

➢ **Are more suitable for software implementations, because they work with blocks of data which is usually the width of a data bus (64 bits).**

➢ **More suitable implemented in software**

❖ Stream Cipher

➢ **Stream cipher treats the message as a stream of bits and performs mathematical functions on them individually**

➢ **Operate on small units of plaintext, bits**

➢ **Symmetric encryption**

➢ **Usually implemented in hardware**

➢ **Encrypts by operating on a continous data stream**

➢ **Some stream cipher use stream generator**

➢ **Statistically unpredictable**

➢ **Much faster than any block cipher**

➢ **Effective Stream algorithm contains**

- **Long periode of no repeating patterns within keystream values**
- **Statistically unpredictable**
- **The keystream is not linearly related to the key**

❖ One Time Pad Vernam Cipher

➢ **Invented 1917 by the US Army Signal Corps and AT&T**

➢ **Is unbreakable and each pad is used exactly once**

➢ **Key only used once and never again**

➢ **The random key is the same size as the message**

➢ **Add modulo 26 to a letter**

➢ **Not OK for BIG messages**

➢ **Key must be completely random**

❖ Book or Running-key cipher

➢ **Uses steps in the physical world around us, like books (page, line number and word count).**

➢ **Each word is described by a sequence of numbers.**

➢ **Breaks a message into fixed length**

➢ **Operate on fixed size blocks of plain text**

➢ **The key can be paragraph / page number etc**

- **Best on general-purpose computer**
- **Attack: Redundancy in the key**

❖ Clipper Chip

- **A NSA designed tamperproof chip for encrypting data**
- **The Clipper chip contains the Skipjack encryption algorithm.**
- **Each chip contains a unique 80-bit unit key U, which is escrowed in two parts at two escrow agencies**
- **The unit key is stored in the database under this serial number.**
- **The sending Clipper Chip generates and sends a Law Enforcement Access Field (LEAF) value included in the transmitted message**
- **Based on a 80-bit key and a 16-bit checksum.**
- **Was en encryption chip the US government wanted to implement into many American made devices so that they could listen to communication that contained suspected information**
  - **A.) fax machines**
  - **B.) telephones**
  - **C.) modems**
  - **NOT IN computer networks**
- **Clipper Chip - implemented in tamper proof hardware**
- **Each clipper chip has a unique serial number and an 80 bit unique unit or secret key.**
- **The Clipper Chip use The skipjack secret key algorithm which was developed by the NSA to enable the government to decrypt any traffic encrypted using the clipper chip**
- **The chip is manufacture so that it cannot be reverse engineered**
- **The problem with the clipper chip is that it has too weak a key at 80 bits and it has no public scrutiny.**

❖ Key Escrow

- **The unit keys are split into two sections and are given to two different escrow agencies to maintain**
- **Different agencies or entitles, hold onto the different pieces and come together when decryption is necessary**
- **Key scrow is a practice that splits up the necessary key required to decrypt information**
- **Allowing law enforcement to obtain the keys to view peoples encrypted data**
- **Court order to get both pieces**
- **The escrowed encryption standard is embodied in the US governments Clipper Chip,**
- **The 80 bit key of the clipper chip is weak.**
- **Key escrow is mainly used when hardware encryption chips**
- **Key escrow approach is fair cryptosystems.**

- **Used when hardware encryption chips are used**

❖ Fair cryptosystems

- **Fair cryptosystems, Separate the necessary key required for decryption this methode**
- **Take place in the software encryption processesusing public key cryptography**
- **Here, the private key of a public/private key pair is divided into multiple parts and distributed to different trustees.**

❖ Steganography

- **Steganography (from Greek steganos, or "covered," and graphie, or "writing"**
- **Hiding data in another message so that the very existence of the data is concealed**
- **The least significant bit of each word can be used to comprise a message without causing any significant change in the image**
- **A message can by hidden in:**
  - **A wave file**
  - **A graphic file**
  - **Unused spaces on a hard drive**
  - **Sectors that are marked as unusable**