Yusuf Selaboy

VUG/CSC/21/5772

Cyber security

9th May, 2024.

1. **Vigenère Cipher**

Vigenere Cipher is a method of encrypting alphabetic text. It uses a simple form of polyalphabetic substitution. A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. The encryption of the original text is done using the Vigenère square or Vigenère table.

**Example:**

Input : Plaintext : GEEKSFORGEEKS

Keyword : AYUSH

Output : Ciphertext : GCYCZFMLYLEIM

For generating key, the given keyword is repeated

in a circular manner until it matches the length of

the plain text.

The keyword "AYUSH" generates the key "AYUSHAYUSHAYU"

* **Hill Cipher**

Hill cipher is a polygraphic substitution cipher based on linear algebra.Each letter is represented by a number modulo 26. Often the simple scheme A = 0, B = 1, …, Z = 25 is used, but this is not an essential feature of the cipher. To encrypt a message, each block of n letters (considered as an n-component vector) is multiplied by an invertible n × n matrix, against modulus 26. To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption.

The matrix used for encryption is the cipher key, and it should be chosen randomly from the set of invertible n × n matrices (modulo 26).

Examples:

Input : Plaintext: ACT

Key: GYBNQKURP

Output : Ciphertext: POH

Input : Plaintext: GFG

Key: HILLMAGIC

Output : Ciphertext: SWK

* **Implementation of Vernam Cipher or One Time Pad Algorithm**

One Time Pad algorithm is the improvement of the Vernam Cipher, proposed by An Army Signal Corp officer, Joseph Mauborgne. It is the only available algorithm that is unbreakable(completely secure). It is a method of encrypting alphabetic plain text. It is one of the Substitution techniques which converts plain text into ciphertext. In this mechanism, we assign a number to each character of the Plain-Text.

The two requirements for the One-Time pad are;

* The key should be randomly generated as long as the size of the message.
* The key is to be used to encrypt and decrypt a single message, and then it is discarded.

So encrypting every new message requires a new key of the same length as the new message in one-time pad.ax

The ciphertext generated by the One-Time pad is random, so it does not have any statistical relation with the plain text.

The assignment is as follows:

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F | G | H | I | J |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| K | L | M | N | O | P | Q | R | S | T |
| 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |
| U | V | W | X | Y | Z | | | | |
| 20 | 21 | 22 | 23 | 24 | 25 | | | | |

1. **Difference between AES and DES ciphers**

**What is AES?**

It stands for Advanced Encryption Standard, developed in 2001. As triple-DES was found to be slow, AES was created and is six times faster than the triple DES. It is one of the most widely used symmetric block cipher algorithm used nowadays. It works on bytes rather than bits.

**What is DES?**

It stands for Data Encryption Standard, developed in 1977. It is a multi-round cipher that divides the full text into 2 parts and then work on each part individually. It includes various functionality such as Expansion, Permutation, and Substitution, XOR operation with a round key.

AES and DES are both examples of symmetric block ciphers but have certain dissimilarities.

|  |  |  |
| --- | --- | --- |
|  | AES | DES |
| 1. | AES stands for Advanced Encryption Standard | DES stands for Data Encryption Standard |
| 2. | The date of creation is 2001. | The date of creation is 1977. |
| 3. | Byte-Oriented. | Bit-Oriented. |
| 4. | Key length can be 128-bits, 192-bits, and 256-bits. | The key length is 56 bits in DES. |
| 5. | Number of rounds depends on key length: 10(128-bits), 12(192-bits), or 14(256-bits) | DES involves 16 rounds of identical operations |
| 6. | The structure is based on a substitution-permutation network. | The structure is based on a Feistel network. |
| 7. | The design rationale for AES is open. | The design rationale for DES is closed. |
| 8. | The selection process for this is secret but accepted for open public comment. | The selection process for this is secret. |
| 9. | AES is more secure than the DES cipher and is the de facto world standard. | DES can be broken easily as it has known vulnerabilities. 3DES(Triple DES) is a variation of DES which is secure than the usual DES. |
| 10. | The rounds in AES are: Byte Substitution, Shift Row, Mix Column and Key Addition | The rounds in DES are: Expansion, XOR operation with round key, Substitution and Permutation |
| 11. | AES can encrypt 128 bits of plaintext. | DES can encrypt 64 bits of plaintext. |
| 12. | It can generate Ciphertext of 128, 192, 256 bits. | It generates Ciphertext of 64 bits. |
| 13. | AES cipher is derived from an aside-channel square cipher. | DES cipher is derived from Lucifer cipher. |
| 14. | AES was designed by Vincent Rijmen and Joan Daemen. | DES was designed by IBM. |
| 15. | No known crypt-analytical attacks against AES but side channel attacks against AES implementations possible. Biclique attacks have better complexity than brute force but still ineffective. | Known attacks against DES include Brute-force, Linear crypt-analysis, and Differential crypt-analysis. |
| 16. | It is faster than DES. | It is slower than AES. |
| 17. | It is flexible. | It is not flexible. |
| 18. | It is efficient with both hardware and software. | It is efficient only with hardware. |

1. **Difference between AES and RSA Encryption**

Encryption in cryptography is a process by which a plain text or a piece of information is converted into cipher text or a text which can only be decoded by the receiver for whom the information was intended.

**Advanced Encryption Standard (AES)**

AES, a symmetric key encryption method developed by Belgian cryptographers Joan Daemen and Vincent Rijmen, was presented by NIST in 2001. Rijndael secures critical data in communication networks, financial transactions, and file storage. AES supports 128-bit data blocks and 128, 192, or 256-bit keys. Substitutions, permutations, and mixing are used to secure encryption. The transmitter and receiver share a key for symmetric encryption. Alice and Bob must securely exchange a secret key before sending an AES-encrypted message. Bob can decrypt the message using the same secret key.

**Rivest-Shamir-Adleman (RSA)**

Ron Rivest, Adi Shamir, and Leonard Adleman invented RSA in 1977. This encryption uses huge prime numbers and the difficulty of factoring large composite numbers. RSA encrypts and decrypts using public and private keys. The public key is disclosed, but the secret key is concealed. This enables keyless secure communication. Bob’s public key lets Alice send Bob an RSA-encrypted message. Bob’s private key decrypts the message. Digital signatures and key exchange use RSA. RSA is slower than AES and unsuitable for big data encryption owing to its computational complexity.

**Difference between AES and RSA Encryption**

|  |  |  |
| --- | --- | --- |
| **Attribute** | **AES** | **RSA** |
| Type | Symmetric key encryption | Asymmetric (public key) encryption |
| Key Length | 128, 192, or 256 bits | 1024, 2048, or 4096 bits (common) |
| Speed & Efficiency | Fast and efficient for bulk data | Slower, not suited for large data |
| Use Cases | Encrypting files, databases, and channels | Key exchange, authentication, signatures |
| Encryption Process | Substitution-permutation network | Modular exponentiation |
| Key Distribution | Requires a secure method to share the secret key | No need to securely share the public key |
| Computational Complexity | Relatively low | High, especially for large key lengths |
| Attack Resistance | Vulnerable to brute-force attacks, but still secure | Vulnerable to advances in factoring techniques |
| Key Management | Easier, as only one key is involved | More complex due to separate public and private keys |
| Suitability for Hardware | Well-suited for hardware implementation | Hardware implementation can be more challenging |
| Quantum Resistance | Vulnerable to quantum attacks (e.g., Grover’s algorithm) | Potentially vulnerable to quantum attacks |
| Example | Secure file storage and communication | Secure email and digital certificates |

1. **Steganography**

Steganography can be defined as the practice of representing information within another message or physical object, in such a manner that the presence of the information is not evident to human inspection. In computing/electronic contexts, a computer file, message, image, or video is concealed within another file, message, image, or video.

The first recorded use of the term was in 1499 by Johannes Trithemius in his Steganographia, a treatise on cryptography and steganography, disguised as a book on magic. Generally, the hidden messages appear to be (or to be part of) something else: images, articles, shopping lists, or some other cover text. For example, the hidden message may be in invisible ink between the visible lines of a private letter. Some implementations of steganography that lack a formal shared secret are forms of security through obscurity, while key-dependent steganographic schemes try to adhere to Kerckhoffs's principle.

The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable they are, arouse interest and may in themselves be incriminating in countries in which encryption is illegal. Whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing both the fact that a secret message is being sent and its contents.

**Techniques of Steganography**

**Physical**

Placing the message in a physical item has been widely used for centuries. Some notable examples include invisible ink on paper, writing a message in Morse code on yarn worn by a courier, microdots, or using a music cipher to hide messages as musical notes in sheet music.

**Social steganography**

In communities with social or government taboos or censorship, people use cultural steganography—hiding messages in idiom, pop culture references, and other messages they share publicly and assume are monitored. This relies on social context to make the underlying messages visible only to certain readers. Examples include:

* Hiding a message in the title and context of a shared video or image.
* Misspelling names or words that is popular in the media in a given week, to suggest an alternate meaning.
* Hiding a picture that can be traced by using Paint or any other drawing tool.[citation needed]

**Digital messages**

Since the dawn of computers, techniques have been developed to embed messages in digital cover mediums. The message to conceal is often encrypted, then used to overwrite part of a much larger block of encrypted data or a block of random data (an unbreakable cipher like the one-time pad generates ciphertexts that look perfectly random without the private key).

Examples of this include changing pixels in image or sound files, properties of digital text such as spacing and font choice, Chaffing and winnowing, Mimic functions, modifying the echo of a sound file (Echo Steganography).[citation needed], and including data in ignored sections of a file.