|  |
| --- |
| Marco Cavani |
| Assessment 1 Portfolio CSI2108 Cryptographic concept |
| 10570027 |

|  |
| --- |
| Marco CAVANI  4-14-2022 |

Contents

[Stream cipher 2](#_Toc100857172)

[Encryptions stream cipher 2](#_Toc100857173)

[Decryption ciphertext 2](#_Toc100857174)

[Security of the stream cipher 2](#_Toc100857175)

[block cipher 2](#_Toc100857176)

[Stream cipher vs Block cipher (symmetric encryption) 3](#_Toc100857177)

[Stream cipher vs trivium 4](#_Toc100857178)

[Demo Block Cipher 4](#_Toc100857179)

[Data Encryption Standards DES 4](#_Toc100857180)

[The Advanced Encryption Standard EAS 4](#_Toc100857181)

## Stream cipher

For part one, I have created a JavaScript script that generates random numbers range 33 – 126 to form a numerical keystream based on the length of the plaintext. Additionally, the script converts the keystream to characters as per ascii table and then returns the equivalent of each word within the keystream as 1-byte binary code. The words within the plaintext are also converted to 1-byte binary code. As result, I have an unpredictable keystream generated from a cryptographically secure [pseudorandom number generator](https://marco-criptography-portfolio1.netlify.app/) (CSPRNG). And both, the plaintext and the keystream are switched to binary code.

The key stream must be the same length of the plaintext. To achieve that, the keystream can be repeated as needed. To obtain the ciphertext both plaintext and key are combined inside the XOR function.

### Encryptions stream cipher

The symmetric stream cipher formula is as followed:

x = plaintext | s = Keystream | y = Ciphertext

*y = x + s (mod2) or y = x ꚛ s*

### Decryption ciphertext

y = Ciphertext | s = Keystream | x = plaintext

*x = y + s (mod2) or x = y ꚛ s*

### Security of the stream cipher

1. The key must be generated in an unpredictable way
2. The key must be used only once
3. The key must be transmitted securely

Despite the unpredictability of the sequence in which the keystream is generated, the stream cipher can be vulnerable to letter frequency analysis attack, and Oscar could guess the plaintext by analyzing the frequency of a character within the cipher text.

The ciphertext is easy to compute by knowing the key. In fact, Alice’s message is easily decrypted by Bob which can use the same formula to find out the message. That is way the key must be transmitted securely.

## block cipher

For the block cipher I have used my surname as keystream, first the excel sheet will look at the plaintext which is linked to the look-up table. The look-up table allows us to assign a numeric value to letters respectively to their position on the alphabet e.g., a=0 b=1. Then the first round of permutation will switch the position of the numbers in each block as followed: 123456 to 314265. After that, the substitution round will increment the permuted numbers by 3. then the value of the first key and the numbers obtained from the permutation will be evaluated like so: k2 = a + b (mod26) to form the second key. Soon after, another 2 rounds of permutation and substitution along with the third key are implemented to ensure the security of the cipher. This way, the block cipher will include three rounds of confusion and diffusion along with 3 keystreams. The block cipher is secure as we have implemented three rounds of confusion(substitution) and diffusion(permutation). However, the security of it could be improved by implementing:

* More round of confusion and diffusion
* Key schedule
* S-BOX
* Triple encryption
* Key whitening

## Stream cipher vs Block cipher (symmetric encryption)

In a stream cipher the encryption is made by encrypting a message bit by bit while in a block cipher the encryption is done by encrypting a portion of information. In fact, the plain text in a block cipher, is broke down to a fixed size before converting it to a cipher text. Calendar

Description automatically generated

Figure 1

Figure 1 shows, the plaintext within the block cipher which is separated in 2 chunks. In fact, the block cipher encrypts the entire block which is six characters long with the same key. This means that the encryption of the plaintext depends on every other character within the same block. In contrast with the stream chipper where each bit is encrypted individually along with the key which is the same length of the plaintext. See table below.

|  |  |  |  |
| --- | --- | --- | --- |
| Stream cipher | X = plaintext | S = keystream | Y = ciphertext |
| X1 | X2 | X3 | X4 |
| S1 | S2 | S3 | S4 |
| Y1 | Y2 | Y3 | Y4 |

Furthermore, both stream and block cipher can ensure security over internet communication, and which one is better depends on the usage. For example, the stream cipher tends to be small and computationally easier for software which make it optimal for voice encryption over mobile devices. In contrast with the block cipher which tend to use more computational resources. However, the block cipher is often used to encrypting communications over the internet as it can provides integrity protection, authentication as well as encryption.

## Stream cipher vs trivium

Trivium is a stream cipher that unlike the conventional stream cipher combines multiple linear feedback shift register to produce a secure keystream using an 80-bit vector number to generate the first register. The vector is used only once, and it is mixed up with the key to generate a key stream.

## Demo Block Cipher

|  |  |
| --- | --- |
| Block-size | 48-bits |
| Rounds of confusion & diffusion | 3 |
| Key length | 48-bits |
| Type of cipher | Symmetric block cipher |

The block cipher seen in figure 1, has three rounds of confusion (substitution) and diffusion(permutation), the key length and the block size are both 48-bits.

## Data Encryption Standards DES

|  |  |
| --- | --- |
| Block-size | 64-bits |
| Rounds of confusion & diffusion | 16 |
| Key length | 56-bits/ each round 48-bits |
| Type of cipher | Symmetric block cipher |

The algorithm in DES is initialized with the permutation of the plaintext, then 16 round of confusion and diffusion. Initially, the key stream is reduced from 64-bits to 56-bits. After that the block is divided in two halves of 32-bits each. Then, the right halve is expanded to 48-bits and computed inside the s-box with the key which have now an equivalent length as per key schedule process. As result, the s-box outputs a 32-bits element. The element is combined with the 32-bits on the left halve through a process called XOR. Then the element on the right is swap with the element on the left to initialize the next round.

## The Advanced Encryption Standard EAS

|  |  |
| --- | --- |
| Block-size | 128-bits |
| Rounds of confusion & diffusion | 10 at 128-bits  12 at 192-bits  14 at 256 bits |
| Key length | 128 bits |
| Type of cipher | Symmetric block cipher |

In AES the block-size and the key-length are both 128-bits also there are 10 rounds of confusion and diffusion at 128-bits 12 round at 192-bits and 14 rounds at 256-bits. AES is the currently used as standard cipher and provide more security than DES as the key length is greater.