

***CSG2108 Cryptographic Concept***

***Assignment 1 : Portfolio - Part 1***

Group 10

Name :

Park kyung tak (1051 3377) (Leader)

Kyae Sin Min Maung (1057 9860)

**Table of Contents :**

[**Encryption of Stream Cipher**](#_qj3ee81yc7l9)3

[**Decryption of Stream Cipher**](#_d73i0kpgbvwi)4

[**Encryption of Block Cipher**](#_80yiggtqydhc)6

[**Decryption of Block Cipher**](#_yuoahhcgb6qu)7

[**Compare and Contrast two symmetric ciphers**](#_fko7ml4243wh)9

[Stream Cipher](#_l12hzfqy4lmc) 9

[Block Cipher](#_7mpo0hrrfzs8) 9

[Comparing Stream cipher with Trivium](#_uym33l6hvdg2) 9

[Comparing Block cipher with AES](#_uym33l6hvdg2) 10

[Which is easier to use.](#_vlmz55mq6tmb) 10

[Which is more secure.](#_equm3ug94cny) 10

[Which cipher to use in a given situation.](#_yum3z8eluaxo) 11

Excel spreadsheet

[Cryptographic Concept - Portfolio part1 excel spreadsheet](https://docs.google.com/spreadsheets/d/1KqB7H0MkhtBffPePpxcnt969rQSeMib4-NM3ULWYf-w/edit?usp=sharing)

*\*\*The ciphers are made with MS excel file.\*\**

# **Encryption of Stream Cipher**

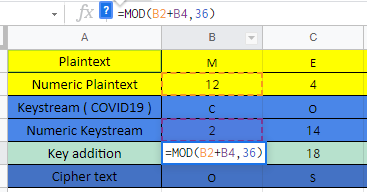
Designing own stream cipher to encrypt the message X. (The message X is ‘Meet Alice next to the fridge in Building 18 at ECU Joondalup campus.’). Stream cipher excel sheet composition is ‘lookup table’, ‘stream cipher (encryption)’, and ‘stream cipher (decryption)’.

We’ve decided to create the keystream with the key ‘COVID19’. Because the keystream must be unpredictable and the key should not contain continuous alphabets or numbers. ‘COVID19’ is the key that does not contain all of the conditions that is not required.

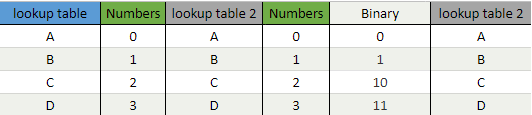
The principle of stream cipher is to substitute the plaintexts with numbers through the ‘lookup table’ that we put on the spreadsheet. Also, we need to substitute the keystream into numbers which is ‘COVID19’.

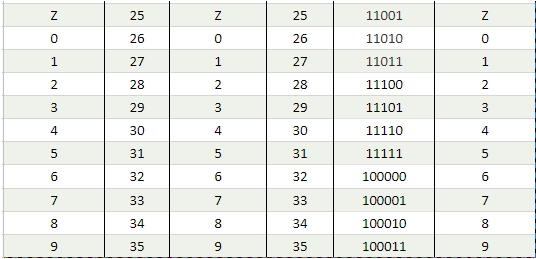
And then, we use the formula  to XOR and encrypt the substituted plain text into ciphertext, which is ‘mod ( [substituted plaintext] + [substituted keystream] , 36)’ in this sheet.





*“The formula must be mod 36, because lookup table contains alphabets and numbers”*





After we gets the key addition through mod36, we substitute them into an Alphabets and then we gets the ciphertext what Alice sent to Bob by stream cipher. We used ‘=VLOOKUP()’ formula on excel to put the data from lookup table.

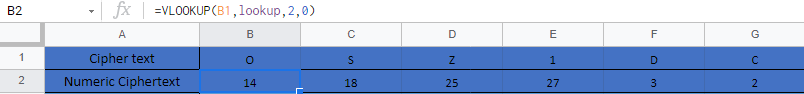
*(\*\* ‘=VLOOKUP()’ is explained on video.)*



# **Decryption of Stream Cipher**

On excel ‘stream cipher (decryption)’ spreadsheet, it shows how to decrypt the stream cipher that Alice sent to Bob. In a simple way to explain, it is only done in the opposite way of encryption. First, Bob has to substitute the ciphertext and the keystream into numeric by using ‘=VLOOKUP()’ to search the data from the lookup table.

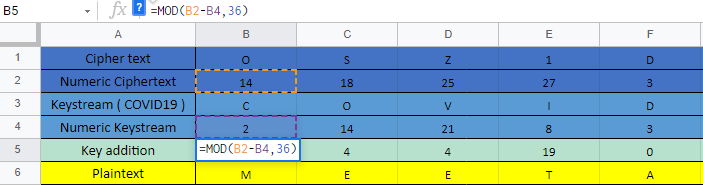
*(\*\* ‘=VLOOKUP()’ is explained on video.)*



Next, in decryption, not like encryption Bob has to use which is exact opposite way with encryption. 

Reason why Bob use the ‘-‘ instead of ‘+’, this formula is the explanation of it.





And then Bob will be able to get the key addition in numbers, and when Bob substitute the key addition through lookup table, he will get the plaintext that Alice sent him.

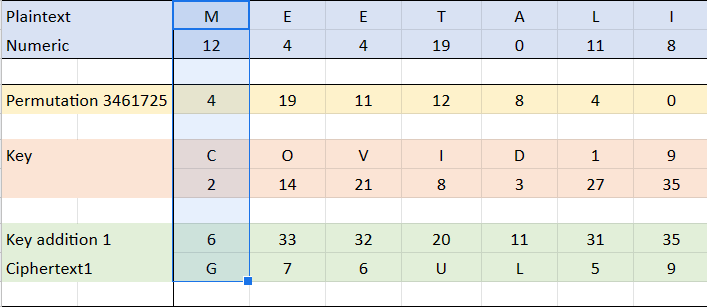


After we made a stream cipher, what I thought is that this encryption could be the most simplest and basic way to encrypt the plaintext. But it is also the most easiest encryption that could be decrypt or attacked by unknown attackers. Because the encryption process is just to substitute the plaintext and the key and XOR them.

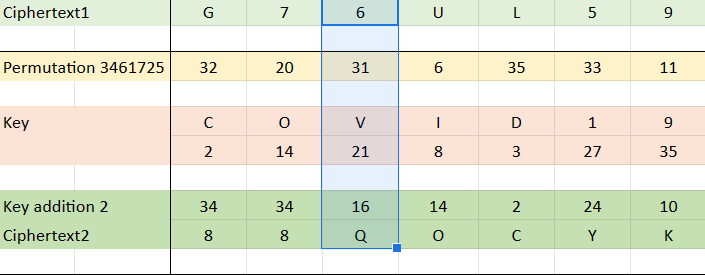
# 

# **Encryption of Block Cipher**

The first part is Block cipher encryption. First of all, we have chosen the key as ‘COVID19’ and the permutation as 1234567 to 3461725. A permutation is just basically rearranging numbers so that the encryption becomes more stable and more secure. The plain text is “Meet Alice next to the fridge in building 18 at ECU Joondalup Campus.’. We have started from zero so M will be 12, E will be 4, T will be 19, and etc. After we added the Key which is 2,14,21,8,3,27,35 and we got the key edition 1, which is the sum of permutation numbers and key numbers. And then after we get the result, we turn those key numbers into ciphertext 1. We named it one because there will be 3 Permutations working simultaneously. So, the first key addition is done and now the 2nd permutation starts. The next step is to change that result to permutation numbers.



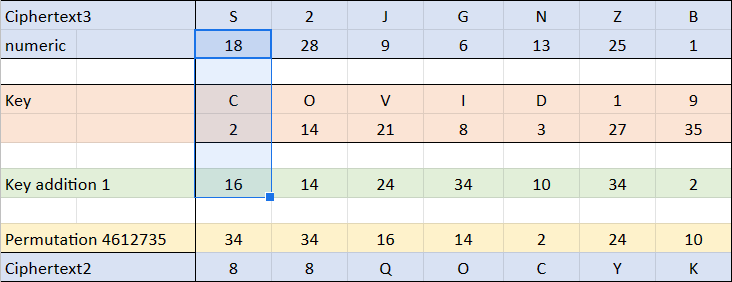
The addition of key and permutation numbers aren't really difficult. But this is where things get tricky. So, if you add 21 and 31 right here. you will get 52 which is not in the lookup table.



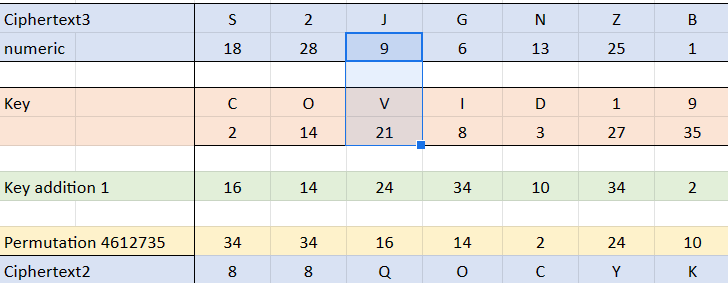
The lookup table ends with 35. So, to continue, we have to start all over from zero. And then count our way to 52. It adds up to 16 which is the letter “Q”. That is the only difficult part that we have to think through and the others which don't exceed 35 all work out perfectly. And then we do another key addition and permutation just like the method from above so that we can get key addition 3. So, three times permutation and encryption is completed.

# **Decryption of Block Cipher**

The next part is the Decryption of block cipher. So, the same as usual, the key will be ‘COVID19’ and the permutation is now changed, which is 4,6,2,7,3,5. We take the ciphertext we got from the encryption and turn it into a numeric value. The key doesn’t change. And now instead of addition, we use subtraction. 18 - 2 is 16 and then rearrange those key addition numbers. Later, we started permutation and turned those numbers to ciphertext 2. After that, we used the key again.



Now, this part is a little difficult because we cannot Subtract 9 - 21.



So, let's use that method from encryption, 9 is basically 45, of which we continued counting from 35. So, we can use 45 - 21. And the result is 24.

And after that, permutate that key addition 2. And turn that. permutation number to ciphertext 2. We can use the same method to get ciphertext 1. And then use the key numbers again. After 3 times, if we turn the last permutation into plaintext, the result will be the same as the start of the block cipher encryption. So, this is how we encrypt a message using the block cipher method, DES.

# **Compare and Contrast two symmetric ciphers**

## *Stream Cipher*

(takes a short time to crack but has its own price.)

* fast and used casually.
* easy to encrypt and takes only a while
* could be vulnerable if used incorrectly.
* used in small companies.
* Security Level - ( High )

## *Block Cipher*

(brute-force attack is the only way to crack it, not famously used)

* slow but has strong security
* difficult to encrypt
* takes a long time to encrypt
* requires more memory
* used in military and highly classified associations.

## *Comparing stream cipher with Trivium*

Trivium is a stream cipher that is arranged in a circle with three different shift registers and each register is connected. It is a fast and efficient cipher that creates a strong keystream by using an 80-bit key. Trivium creates the keystream through XOR and AND gates. But our stream cipher didn’t use the RNG to create the keystream. So the trivium is much more secure than our stream cipher.

## *Comparing block cipher with AES*

First of all, please keep in mind that AES encryption is far more stable and far more secure. AES is used all over the world and it’s very popular. The only downside of using AES is that it takes a lot of space. And also in the DES encryption, if we edit more than three rounds of encryption and key addition, we can make this more secure.

## *Which is easier to use.*

In comparing and contrasting two symmetric ciphers, we personally think that stream ciphers are easier to create and faster to run. Because stream cipher doesn't require multiple rounds of encryption or decryption. The reason why we say this? It's because there are no permutation layers or anything. We just turn the plaintext into numeric texts and add the key addition. And then turn this into ciphertext. which is, in our opinion, easier to encrypt than block cipher.

## *Which is more secure.*

So, if I have to say which is more secure and why? I would choose Block cipher encryption and decryption method. It's more Secure. If we think deep into the symmetric ciphers, the stream cipher uses the whole sentence and encrypts it with a new sentence. While block ciphers use each block or letter and turn it into ciphertext with multiple rounds. So that's the reason why we think. Block cipher is more secure. In block cipher, to compare with AES, AES is widely used and more efficient than the DES. The only downside of AES is that encryption takes a long time. While the DES encryption can only take up to 2 or 3 hours.

## *Which cipher to use in a given situation.*

So, let's say if you want to encrypt a message faster and don't need much security, then we should use stream ciphers. Stream ciphers are widely used in businesses and companies where cyber-attacks rarely occur. But if the message you want to encrypt is highly important and needs more security, then we should consider using the Block cipher method. AES and DES encryptions are widely used in Military works banking systems and also in classified healthcare systems.