Vigenère and Caesar Symmetric-Key Algorithms

Michael Kokkos, Alexander Soloviev

Aigaleo - Athens, Greece

Abstract

Cryptography is the field of study that deals with the processes of encryption and decryption of data, with the intention to be readable only from authorized recipients. Two main classes of cryptographic algorithms exist, symmetric-key and asymmetric-key. This paper provides the reader with introductory knowledge in the Caesar and Vigenère ciphers, two of the most famous symmetric-key encryption ciphers. Caesar cipher is one of the oldest substitution ciphers. Vigenère cipher is much newer, but is based in the Caesar cipher.

Keywords: Cryptography, Symmetric-key, Caesar's cipher, Vigenère cipher

1. Introduction

The vast expansion of cryptography is one of the major achievements of theoretical computer science. Concepts such as computational indistinguishability, pseudorandomness, and zero-knowledge interactive proofs were introduced [1]. Widely used technologies such as SSL certificates, end-to-end encryption and many others are the pinnacle that the field of modern cryptography offers today. Although the theory and the algorithms that are used in the cryptography field in the current era are fairly complicated they are based on the sound grounds of older and much more simpler ciphers like the ones stated in this paper.

For a long time the term Cryptography was synonymous with encryption. That is the process of conversion of readable data, which are called plaintext, into an unintelligible form, which is called ciphertext [2].

The main goal of encryption is to assist other fields of information security and help users and parties with their confidentiality, integrity and availability of their data (the CIA triad) [3].

2. Categories of Cryptography

Cryptography splits in two main categories, Symmetric and Asymmetric. The factor that differentiates the one from the other is the type of the security key that is used to encrypt or decrypt the data.

This paper's primary focus is two of the most known Symmetric-key ciphers. However a brief introduction in the topic of Asymmetric cryptography will be made.

2.1. Symmetric Cryptography

Figure 1: QR code that leads to the "Introduction to Basic Cryptography: Symmetric Key Cryptography" video, from the channel "Ryan Riley"

Symmetric key cryptography is one of the two main categories of encryption, also it was the only kind of encryption that was publicly known until June of 1976 [4]. The key in Symmetric-key ciphers is the same for encryption and decryption. That means that the sender has to encrypt the data with the same key that the recipient will use to decrypt them, that process is described in Figure 2.

Symmetric cryptography also splits in its own subcategories. There are two types of implementations that exist, the block ciphers and the stream ciphers. This paper will not dive deep into their differences, but the major one is that the block ciphers operate with a fixed transformation on large blocks of plaintext data, in contrary stream ciphers operate with a time-varying transformation on individual plaintext digits [5].

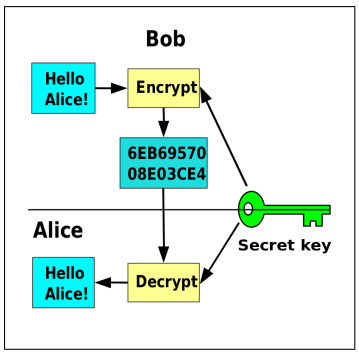

Figure 2: Bob encrypts the plaintext with his secret key. Alice receives the ciphertext and decrypts it with the same key.

Substitution Ciphers: Substitution ciphers utilize the technique of mapping the contents of the cleartext with other content which can include symbols, alphabets or even blocks [6].

Transposition Ciphers: Transposition ciphers are an important subset of classical ciphers. In a transposition cipher the plaintext remains the same, but the order of the characters is shuffled around [7].

2.2. Asymmetric Cryptography

Figure 3: QR code that leads to the "Public Key Cryptography" video, from the channel "Computerphile"

Asymmetric cryptography or Public-key cryptography is the second major category of cryptography, and also the newest one. This method takes a different approach at the problem of encryption and decryption of information. Two keys exist, a public and a private, the public is used for encryption of the plaintext and the private is used for decryption of the ciphertext [8].

The main advantage of this method is that the sender and the recipient don't have to exchange any kind of secret key between them, they only need to exchange their public keys which are public anyway. Examples of asymmetric algorithms are RSA, DSA, ECC, etc [8].

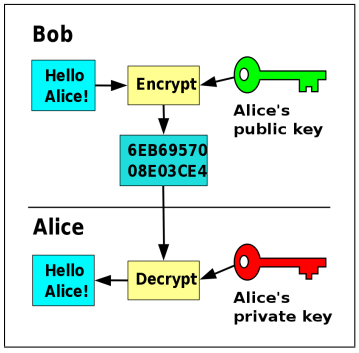

Figure 4: Bob encrypts the plaintext with Alice's public key. Alice receives the ciphertext and decrypts it with her private key.

3. The Caesar's Cipher

Figure 5: QR code that leads to the "Crack the Code: The Caesar Cipher" video, from the channel "Paget Teaches..."

The Caesar cipher technique is one of the oldest methods of encryption. The process is the following, every character in a given plaintext is replaced by a letter with constant number of positions down the letter. A special case of Caesar's cipher is the ROT13 cipher, which is the Caesar's cipher with a shift of 13, and its primary use is to hide spoilers, offensive content, etc.

For example, consider that we want to encrypt the message "HELLO" with a shift of 3. The ciphertext would be "KHOOR". Because "H" is the 8th letter of the english alphabet, and we are adding the shift which is 3 we are getting as a result the 11th letter of the English alphabet, which is "K". The same process is followed for the rest of the plaintext. If there are not any more letters, the process is beginning from the start with a modulo logic, for the example above, if the letter "Z" was present, the equivalent ciphertext would be "C".

The mathematical formula for the process of enciphering is given below:

$$e_n(x) = (x + n) mod 26 \tag{1}$$

Where "x" is the plaintext character to be enciphered and "n" is the shift, mod26 is used because the English language uses a twenty-six letter alphabet, if another alphabet or set of characters is used it has to be changed accordingly.

Similarly the deciphering is presented as:

$$d_n(x) = (x - n) mod 26 \tag{2}$$

4. Vigenère cipher

Figure 6: QR code that leads to the "Vigenere Cipher Explained (with Example)" video, from the channel "Aladdin Persson"

The Vigenère cipher is a method of encryption that uses multiple Caesar ciphers to encipher the plaintext using a keyword. It is a form of polyalphabetic substitution and took it's name after its inventor Blaise de Vigenère.

The cipher was considered unbreakable for some three hundred years, where Friedrich Kasiski published a general method of breaking Vigenère ciphers [9].

The encryption process can be described with the following formula:

$$C_i = EK(P_i) = (P_i + K_i) mod 26 \tag{3}$$

Where "C" is the ciphertext, "E" is the Vigenère encryption and "K" is the key.

The deciphering process can be described as:

$$P_i = DK(C_i) = (C_i - K_i) mod 26 \tag{4}$$

Where "P" is the plaintext and "D" is the Vigenère decryption.

There is also an alternative to the mathematical formulas that are described above, and it's called the Vigenère square.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figure 7: The Vigenère square.

4.1. Encryption Process

The theory above can be applied to the following example. The plaintext to be encrypted is "HELLOWORLD", and the keyword that is to be used for the encryption is "KEY".

The first step for the person sending the message is to repeat the keyword until it matches the character length of the plaintext message. For the case that is being studied, this will be "KEYKEYKEYK".

Now the person who wants to encrypt the message would refer to the Vigenère square, to produce the final ciphertext. The first letter is "K" and the plaintext letter is "H", so the person would go to the "K" column and find the letter that corresponds to it. It is easy to spot that this would be the letter "R".

The next letter is "E" and the plaintext is "E" too, so the produced letter would be "I". The process will go on until the person gets the final ciphertext. That would be "RIJVSUYVJN".

4.2. Decryption Process

The recipient who will decrypt the message would follow a somewhat similar process. First, the ciphertext characters will be replaced by the key-phrase repeatedly ("KEYKEYKEYK"), and then by matching the letters from the ciphertext in the rows with the correspondent columns, the plaintext will be unveiled.

5. Conclusions

Conclusions from the course of encrypting data using the Caesar and Vigenère ciphers, is that although they are obsolete with today's standards, they are a great introduction into the fairly complex topic of cryptography.

References

[1] O. Goldreich, Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali, 1st ed., Association for Computing Machinery, 2019.

[2] D. Kahn, The Codebreakers – The Story of Secret Writing, 1st ed., The Macmillan Company, 1967.

[3] S. Samonas, D. Coss, The CIA Strikes Back: Redefining Confidentiality, Integrity And Availability In Security, Journal of Information System Security 10 (2014) 21–45.

[4] W. Diffie, M. Hellman, New directions in cryptography, IEEE Transactions on Information Theory 22 (1976) 644–654.

[5] G. Simmons, Contemporary Cryptology, The Science of Information Integrity, 1st ed., IEEE Press, 1992.

[6] D. Venkata Vidya Deepthi et al, Proc. International conference on computer vision and machine learning (Journal of Physics: Conference Series, Andhra Pradesh, India, December 2018), volume 1228 of *Lecture Notes in Computer Science*, IOP Publishing, 2019. doi:10.1088/1742-6596/1228/1/012014.

[7] M. Sokouti, B. Sokouti, S. Pashazadeh, An approach in improving transposition cipher system, Indian journal of science and technology 2 (2009) 9–15.

[8] M. Al-Shabi, A survey on symmetric and asymmetric cryptography algorithms in information security, International Journal of Scientific and Research Publications 9 (2019) 576–589. doi:http://dx.doi.org/10.29322/IJSRP.9.03.2019.p8779.

[9] S. Darma Nasution, G. Ginting, M. Syahrizal, R. Rahim, Data security using vigenere cipher and goldbach codes algorithm, International Journal of Engineering Research Technology 6 (2017) 360–363.