SCHOLEDGE International Journal Of Multidisciplinary & Allied Studies
ISSN 2394-336X, Vol.07, Issue 02 (2020)
Pg 30-44.
Paper URL: link.thescholedge.org/1209

SCHOLEDGE Publishing Worldwide
www.theSCHOLEDGE.org
Email: editorial@thescholedge.org
©Publisher

Cryptography and Network Security: A Historical Transformation

Sanjay Kumar Pal
NSHM College of Management and Technology, Kolkata, India.

Dr. Bimal Datta
Budge Budge Institute of Technology, Kolkata, India.

Dr. Amiya Karmakar
Maulana Abul Kalam Azad University of Technology, Kolkata, India.

ABSTRACT

Information is any sort of data and the security of the data is the primary need in the digitized world. Information security alludes to defensive digital protection gauges that are applied to counteract unauthorised access to PCs, individual databases and websites. These capacities fall under cryptography. Cryptography gives clients different kinds of functionalities for hiding the information and validates the clients who utilize the encoded information. All the more officially, Cryptography is a study of ensuring information. This paper speaks to a course of events of the advancement of cryptography from early Egyptian cryptography to the current cryptography encryption strategy and technology. This paper clarifies why we required encryption, why each world leader utilized encryption and why regardless we required it. The procedures utilized during 1899 BCE and the methods till now as the security is the significant piece of the correspondence on the computerized world thus compose this paper to tell all people, groups what various sorts of cryptography strategies utilized in various time of times. Furthermore, this paper will help people groups as researchers to know in insights concerning the diverse cryptographic machines and their work and proficiency in encrypting information of those machines.

Keywords: Cryptography, Encryption, Decryption, Cipher, Ciphertext, Plaintext, Data Security.

1.0 Introduction

The earliest known use of cryptography is found in non-standard hieroglyphs carved into the wall of a tomb from the Old Kingdom of Egypt circa 1900 BC. At the start of cryptology, it was just verifying a snippet of data during it was moving between various places composing of a straightforward message so that the composed data is secured. The word "cryptography" is originated from the Greek words 'Kryptos', which implies the secret and graphos, which means composing as recommended by(Waqiyuddi, Zulkifli,2007)[1] which implied covered up and composing (Katz et al., 1996). It was exclusively utilized for concealing the message, they convert the data into various incomprehensible groups of information to ensure the substance of the messages [6]. It was done with the goal that nobody knows the data during the time it is been conveyed from source to goal. In the digital era, cryptography isn't just for essential message secrecy, however, now it additionally incorporates a few portions of message sender/beneficiary uprightness checking computerized marks and character verification in addition to other things. During the twentieth century where encryption is utilized in political and military settings more the need to disguise messages in codes and went around is more prominent with the goal that foes can't disentangle the substance. When there were various groups or clans the need to neutralize each other raised and was flourished alongside the rank savagery, individual's control, and secret. In the support of progress, we found the basic form of cryptography. This likewise incorporates the locales right now included by Egypt, Greece, and Rome.

2.0 Terminology

2.1 Plaintext: The text which is used in cryptography before encryption of message or after decryption of the message.

2.2 Ciphertext: The text which is seen after encrypting the message is termed as ciphertext.

2.3 Encryption: Encryption is the method by which plaintext or any other type of data is converted from a readable form to an encoded version that can only be decoded by another entity if they have access to a decryption key[20].

2.4 Decryption: Decryption is a method by which an encoded text is converted into a readable or understandable format.

2.5 Key: A key is a combination of bits which is used to convert the plaintext to ciphertext or vies -versa.

2.6 Symmetric Algorithm: The symmetric algorithm is one in which the encryption and decryption key are the same.

2.7 Asymmetric Algorithm: An asymmetric algorithm is an algorithm in which the key used in encryption is different from that of the key used decryption. It is also known as public-key cryptography[20].

3.0 Cryptographic Evolution Timeline: This theme contains the pre-innovation utilized in cryptography, post-innovation in cryptography and the cutting edge innovation of cryptography subtleties are as pursue,

3.1 The Oldest Cryptographic Techniques (4000-500 B.C)

In the old occasions, Egyptians began composing kneads in symbolic representation known as "hieroglyph"[37]. The principal has known proof of cryptographic propose that "hieroglyph" is the most established cryptographic procedure which is found in Egypt's old realm around 4500 years back, cut into monuments [23]. It was found on the tomb of aristocrat Khnumhotep II in the town Menet. Khufu. The code was a mystery just known to the copyists who used to transmit messages for the benefit of the king. One such pictograph is demonstrated as follows.

Figure 1:Hieroglyph

As per McDonald (2018)[24], around 1900 BC, the copyists of Khnumhotep[38] drew the biography of his lord life in his tomb. While drawing the hieroglyphics they began utilizing various remarkable images/symbols for disguising or clouding the genuine importance of the engravings (figure 2). On present occasions, this arrangement of encoding messages are called a substitution cipher. Hence, a substitution cipher can be characterized as any ciphering framework that substitutes is or replaces one image or character with another to disguise actual implications.

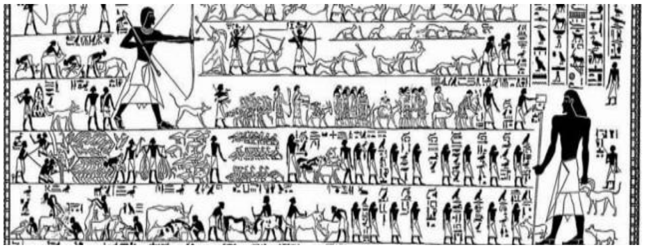


Figure 2: Symbols found in the tomb of Khnumhotep II

This strategy for encryption is very simple for implication but difficult to break for the individuals who could peruse and compose so as the Egyptian culture developed, the substitution of 'hieroglyphic' turned out to be progressively fundamental. There are a few reasons why Egyptians utilizes pictograph encryption framework. They may clutch the holy strategy for their holy ceremonies from ordinary citizens. This strategy for encryption isn't restricted to the Egyptians; it tends to be found in Greece too.

3.2 Greece Crypto Technique(500 B.C)

During the time of 500 B.C, the Spartans built up an apparatus, which was utilized to send and received encoded messages. This gadget is known as "Scytale"[25,39]. This encryption framework was composed on the bars of woods with equivalent radius, a narrow parchment wound on the bar and on the abutting edges, the message was composed. When somebody loosened up the material, the message can't be deciphered. So as to interpret the message and indistinguishable cylinder was required otherwise the letters would not arrange in the way to be perused.

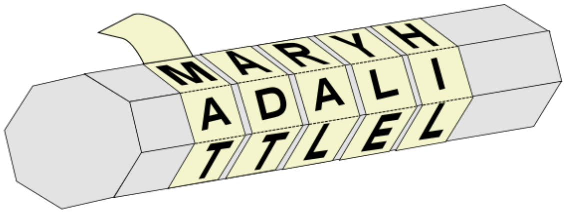


Figure 3: Scytale

For the standard of the modern age, a Scytale can be effectively deciphered but 2500 years back the quantity of individuals who can peruse is handing-off little, the Scytale gives the Spartans a dependable method for moving information starting with one place then onto the next.

3.2.1 Caesar Cipher Method:

Caesar Cipher is a shift cipher it is otherwise called Caesar shift. It is one of the simplest and most commonly known encryption procedures. Its principal work is to supplant each letter of plaintext by some fixed situation beneath the letters in order. For instance, if the left shift of 3 is taken then the alphabet D would be replaced by alphabet A and alphabet E would replace to alphabet B and so on will continue until the plaintext is completely replaced[14,40].

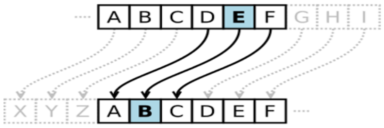


Figure 4: Caesar cipher

3.3 Roman Cryptography Technique:

Greece as well as in Roman we see a significant utilization of cryptology. Right around 2,000 years back Julius Caesar utilizes cryptography to speak with his soldiers. Caesar, being the commander of his soldiers he needs a secured method to speak with his soldiers, accordingly he builds up a technique for encoding messages; the strategy is known as Caesar cipher. Most of the time the messenger carrying the secret message gets captured by the enemy by encrypting the message it stops the enemy from knowing the message even after capturing the messenger; so during the war, it gives the Roman army a huge advantage.

As per McDonald [24], Caesar didn't utilize that mind-boggling type of encryption appeared in figure-4; by some predetermined numbers, he moved the words. This predetermined number is the key to decipher the encrypted code.

3.3.1Polyalphabetic Cipher(1466):

During the mid-1400s a man named Leon Battista Alberti plans an encryption framework with the assistance of a cipher disk. Such a huge number of techniques for substitution opened with the utilization of this mechanical gadget with sliding. The poly-alphabetic cipher[41] is based upon this idea, which speaks to an encryption strategy that experiences a few substitution ciphers all through encryption. David Kahn calls Alberti "the dad of western cryptology" in his book "The Codebreakers"(Kahn 1967)[2]. Alberti was never the built-up his cipher plate idea. A man named Blaise De Vigenere built up a cipher with the assistance of Alberti's poly-alphabetic cipher style in late 1500 which is referred to as Vigenere Cipher. The Vigenere cipher's working principle is nearly equivalent to Caesar cipher just with the exemption that throughout the encryption procedure it changes the key. A grid of letters is utilized in the strategy for substitution which is known as Vigenere Square or a Vigenere Table[42]. The grid that is made of 26 letters in order offset from one another by one letter.

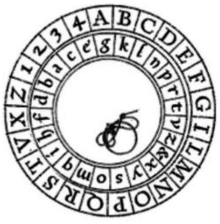
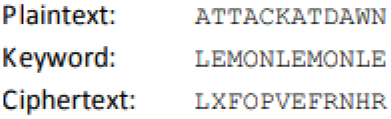


Figure5: Polyalphabetic Cipher

So as to transform one key to another, an uncommon mystery word can be picked. The general guideline is given in the paper “Past Present and Future Method of Cryptography and Data Encryption”, by Nicholas G. McDonald[24]. To substitute the main letter of the plaintext is subbed with the unique mystery word on the x-pivot. Presently rehash this technique for every one of the letters, the recently framed word is rehashed. For example, if the plaintext that must be scrambled is ATTACKATDAWN a mystery word like

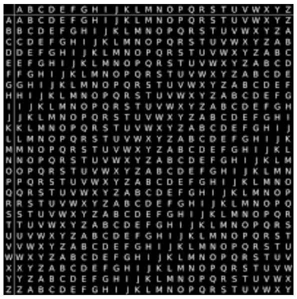
"LEMON" is rehashed like LEMONLEMONLE until the length of the first word is shaped tallying the letters.



Plaintext: ATTACKATDAWN

Keyword: LEMONLEMONLE

Ciphertext: LXFOPVEFRNHR



	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 6:Vigenere Square

3.4 The Semaphore Telegraph(1793):

Semaphore Telegraph[43] is an arrangement of passing on data by methods for the visual sign, utilizing towers with pivoting shutters, also known as blades or paddles. It was developed in the year 1792 in France by Claude Chappe[30]. In this method, the administrators of the pinnacle would watch the closest pinnacle through a spyglass and when the semaphore's arms started to turn-illuminating a message, they would give the message to the following pinnacle, this is the means by which the message move between various towers was done in this instrument the snippets of data is encoded by the situation of the mechanical components. It is a lot quicker than post riders in passing on the message over long separations.

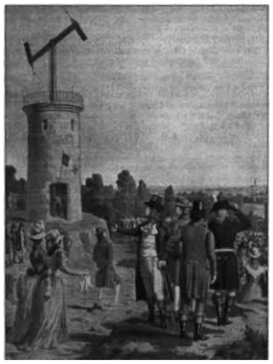


Figure 7: Semaphore Telegraph

3.5Jefferson Disk (1795):

Late 1700's, Thomas Jefferson thought of a cipher framework exceptionally much the same as the Vigenere Cipher with the exception with higher security. His innovation was a framework with 26 wheels, which contains letters in order, which are dispersed haphazardly on each wheel. The wheels were numbered and ordered with a predetermined mandate. This request is the way into the encryption algorithm[1,24]. The messages that will be encrypted are made on the wheels by arranging the wheels with the end goal that the message is available. Some other lines other than the arranged line, which contains the message, is the cipher content. So as to decode the message on the less than desirable end, the individual has to know the best possible request of the wheel. The plain text is arranged elsewhere on the wheels as the cipher content is made on the wheels. Visual output can rapidly bring about finding the first content. There is an extremely uncommon possibility for two non-gibberish messages will surface on the plate during decoding. Like Alberti, Jefferson likewise not the man to build up his encryption system [24]. During the mid1900's, with no information about Jefferson's innovation, the United States Army reinvented Jefferson's Wheel Cipher[44]. Just about a hundred years have gone after Jefferson[24], The United States Army utilized this framework from 1923to 1942 (Thinkquest.org 1999).

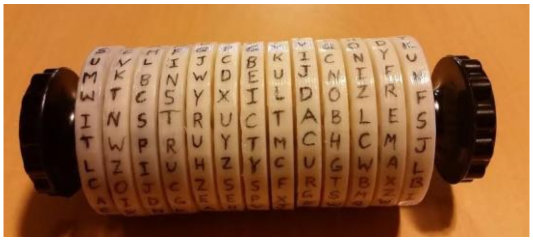


Figure 8: Jefferson Wheel Cipher

3.6 Morse Code(1835):

Morse Code is an encoding plan of characters which is utilized in media transmission. Its principal work is to encode the content characters as institutionalized successions of two unique sign terms called dots and dashes[15]. This Morse code[45] can be retained effectively and its sign is as a sound wave and noticeable light by which it very well may be legitimately deciphered by the gifted people on that field.

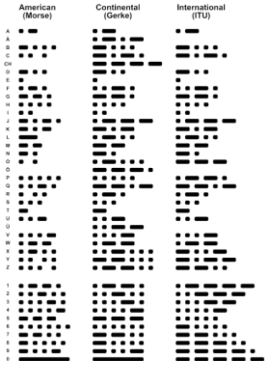

American (Morse)
Continental (Gerke)
International (ITU)

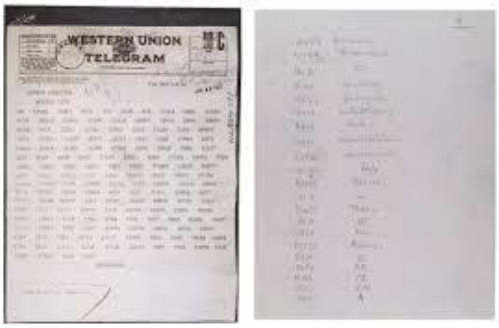
Figure 9:Morse Code

4.0 Cryptography (WW-I):

In this timeframe during World War I, various cryptography methods had been created and the various strategies are as pursue.

4.1 Zimmermann Telegram (1917):

In mid1917 the Zimmerman Telegram, during the beginning periods of World War I, a German encoded telegram reached British cryptographers. This message is frequently referenced as the Zimmerman Telegram[46]. These British cryptographers were able to decrypt the telegram, and in the process of doing so, they changed cryptanalysis history. Utilizing this deciphered message, they had the option to persuade the United States to join the war[1]. The German realm utilizes the Zimmerman telegram as a mystery correspondence between the Foreign Secretary of the German Empire, Arthur Zimmerman, to the German diplomat in Mexico, Heinrich von Eckardt[24]. The wire contained a suggestion for Mexico to recover its region of New Mexico, Texas, and Arizona on the off chance that they backing and join the German reason. Regardless of this offer, Mexico concluded that it would not be possible or even desirable to assume control over its previous regions. World War I was at its stature when the message was sent. Until that point, the United States had endeavored to stay impartial. English, and different partners, had asked for help from the U.S., and frames of mind in the US were gradually moving towards war. The British gave the U.S. the decoded telegram on February 24, 1917, and on April 6, 1917, the U.S. authoritatively proclaimed war against Germany and its allies[24].



WESTERN UNION TELEGRAM

Figure 11: Zimmermann Telegram

4.2 Enigma Machine(1932):

As WWI went on, the US had the issue that they don't have any method for secure correspondence. Pretty much every telephone call made was captured by the Germans, leaving each move made by the partners known to the Germans. Armed force administrator, Captain Lewis concocted an arrangement that used American Indian dialects. He organized a gathering of eight Choctaw men in the unit and guide them to converse with one another over radio and telephone lines. Native American language was extremely significant on the grounds that common codes and figures of a mutual language can be decoded, while codes dependent on an extraordinary language must be contemplated broadly before starting to unravel them. Within 24 hours of utilizing the Choctaw language as encryption, the advantage fell in favour of the United States[24]. Within 72 hours, the Germans were retreating and the allies were in full attack. War Driven Cryptography Enigma Encryption Machine at the finish of World War I, Arthur

Scherbius created the was utilized for encryption and decoding of that permitted up to 10114 potential designs. In light of the various setups, the Enigma was virtually unbreakable with brute force techniques. The first commercially accessible in the 1920s, figure 9, Enigma encryption machine utilized by Nazi Germany It wasn't until World War II that the Enigma picked up its distinction. Because of the Enigma's measurable security, Nazi Germany got pompous about their capacity to scramble secret messages. This arrogance caused the destruction of the Enigma. Along with Enigma had a few worked in shortcomings that Allied cryptographers exploited. The significant shortcoming was that its substitution calculation didn't cryptographers to decode an immense number of ciphered messages sent by Nazi Germans. While the Allied forces were concentrating on splitting the encryption machine called Purple. Rather than the Enigma's rotors, Purple was switches usually utilized for routing phone signals. During the war, the Japanese were generally proficient in annihilating their encryption machines. At present, not one complete Purple machine has been discovered [31].

WWII Enigma Encryption Machine at the finish of World War I, Arthur Scherbius invented the Enigma[47], an electro-mechanical machine that was utilized for encryption and decryption of mystery messages. The Enigma had a few rotors and gears potential designs. As a result of the various setups, the Enigma unbreakable.

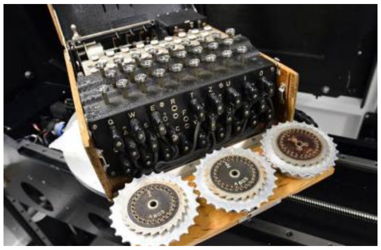


Figure 12:Enigma

5.0 Cryptography for (WW-II):

In this time likewise, unique new cryptography strategies were concocted and the procedures are as pursue.

5.1 Lorenz Cipher:

The Lorenz SZ40, SZ42a, and SZ42b[48] were German rotor stream cipher machines utilized by the German Army during World War II[17]. It was designed to convey at the most significant level in the military. The Lorenz messages made one of the most significant contributions to British Ultra military intelligence and to the allied triumph in Europe in light of its significant level strategic nature of the data.

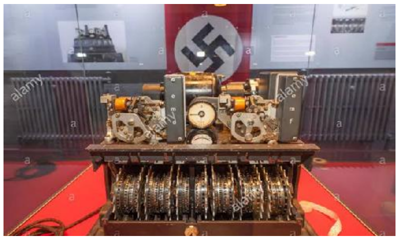


Figure 13: Lorenz Cipher

5.2 SIGABA(1944):

SIGABA is a cipher machine which is utilized for encryption of messages during World War II until the 1950s [18,49]. This is the equivalent encrypting machine that takes a shot at the electromechanical arrangement of rotors yet the change is that it was get enhanced a security perspective than different machines.

Figure 15:SIGABA

6.0 RSA(Cryptosystem):

RSA is a first open key cryptosystem which imagined by three scientists (Rivest-Shamir-Adleman) in 1977[26]. It was generally used to verify the transmission of information. RSA depends on the practical difficulty of the factorization of the result of two enormous prime numbers. The procedure of using RSA, first of all, a user of RSA creates a public key based on two large prime numbers along with auxiliary values and then publishes the key. The prime numbers must be kept secret. RSA is a relatively slow algorithm for encrypting the data so that it is less commonly used.

7.0 Secure Socket Layer(1994):

Transport Layer Security (TLS), and its presently deprecated forerunner, Secure Sockets Layer (SSL), are cryptographic conventions intended to give interchanges security over a PC organize. A few forms of the conventions find across the board use in applications, for example, web perusing, email, texting, and voice over IP (VoIP). Websites can utilize TLS to verify all interchanges between their servers and internet browsers.

8.0 Visual Cryptography(1994):

Visual cryptography[50] was initially presented by M.Naor and A.Shamir on EUROCRYPT in 1994[27]. Visual cryptography is the strategy for encryption that enables visual data to be scrambled so that for decoding it is done precisely no PCs are required. It is utilized in information stowing away, verifying pictures, shading imaging, media and other such fields[22]. Visual Cryptography comes in the field of information hiding utilized in cybercrime, record groups, and so on.

Figure 18:Visual Cryptography

9.0 DeCSS(1999):

DeCSS[51] is a method of decoding content on a commercially delivered DVD video plate. It was the first free PC program. DeCSS's improvement was developed without a permit from the DVD, the association liable for DVD duplicate security was named by Content Scramble System(CSS) utilized by business DVD publishers[29].

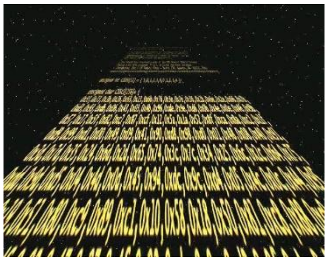
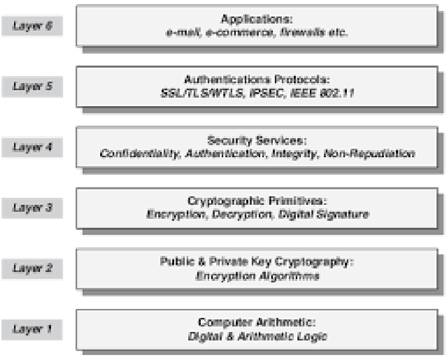


Figure 19:DeCSS

10.0 Modern Cryptography:

In modern Cryptography[52] the accompanying strategies or advances have been mulled over.



Layer 6
Applications:
e-mail, e-commerce, firewalls etc.
Layer 5
Authentications Protocols:
SSL/TLS/WTLS, IPSEC, IEEE 802.11
Layer 4
Security Services:
Confidentiality, Authentication, Integrity, Non-Repudiation
Layer 3
Cryptographic Primitives:
Encryption, Decryption, Digital Signature
Layer 2
Public & Private Key Cryptography:
Encryption Algorithms
Layer 1
Computer Arithmetic:
Digital & Arithmetic Logic

Figure 20: A Six-Layer Model of Information Security Applications

10.1 Secret Key Cryptography:

Mathematically[7], symmetric key cryptosystem[53] can be characterized as the tuple (P,C,K,E,D), where P speaks to the arrangement of limitedly numerous conceivable plain-writings. C speaks to the arrangement of limitedly numerous conceivable figure writings. K speaks to the keyspace, i.e, the arrangement of limitedly numerous potential keys.

$\forall k \epsilon K \exists e_k \in E$(Encryption rule), $\exists d_k \in D$(decryption rule).Each$e_k : P \rightarrow C$ and $d_k : C \rightarrow P$are well-characterized capacities to such an extent that$\forall x \in P, d_k\big(e_k(x)\big) = x$.

Both encryption and decryption keys (which once in a while are similar keys) are stayed quiet and should be known at the two closures to perform encryption or decryption as is appeared in Fig. 21. For encoding/decoding high volume information, Symmetric algorithms are utilized; these algorithms are fast. Symmetric algorithms are classified into two kinds: stream cipher and block cipher.

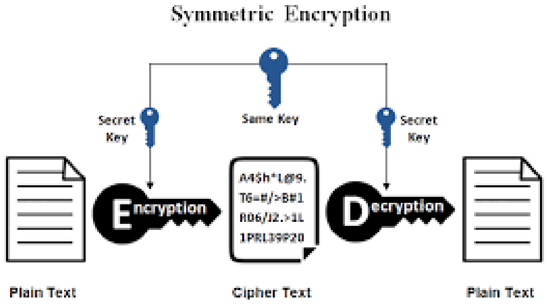


Figure 21:Secret key cryptography

• **Stream ciphers:** One kind of symmetric encryption algorithms is stream cipher in which the input data is encrypted one bit(in some cases one byte) at a time. The encryption of a bit is dependent on the current state that’s why sometimes they are called state cipher. Some of the instances of stream cipher are SEAL, TWOPRIME, WAKE, RC4, A5, and so forth.

• **Block ciphers:** In block cipher algorithm it takes a fixed-length of the block of plaintext as input and transformed it into another block that has a similar length (cipher text) with the assistance of the client gave secret key[33]. The Decryption is done by utilizing reverse conversion to the block cipher content utilizing a similar key. Usually, a block length of 128 bits is utilized in the modern block cipher. Some renowned block cipher is DES, AES, Serpent, RC6, MARS, IDEA, Two-fish, and so forth. The most mainstream block cipher algorithm utilized by DEA (Data Encryption Algorithm); DEAdefined in the standard DES. TDEA utilizes a secret key that has a bit length of 56 bits. It was viewed as protected in the late 1970s, yet the innovation has improved and now can break the DEA in not many hours by propelling brute force attack that is the reason DEA is generally utilized as Triple DEA (TDEA) that may offer security equal to 112 bits. TDEA utilizes three 56-bits keys (in particular K1, K2, and K3). In the event that every one of these keys is autonomously produced, at that point, this is known as the three key TDEA (3TDEA). Nonetheless, if K1 and K2 are independently created, and K3 is set equivalent to K1, at that point, this is known as the two key TDEA (2TDEA). In October 2000, another symmetric cryptographic algorithm "Rijndael" was picked as the new Advanced Encryption Standard (AES) by NIST (National Institute of Standards and Technology). Because of its upgraded 2.3 Hash Functions 21 security level, it is supplanting DEA and triple DEA (TDEA) in a wide scope of uses. Though all previously mentioned secret key cipher offers a high security and computational effectiveness, they likewise show a few disadvantages:

- **Key distribution and exchange:** The master key that is being utilized in this sort of cryptosystems should just be known by the sender and the receiver [34]. Hence, both parties should prevent this key can get compromised by unauthorized entities.
- **Key management:** The system which has numerous clients must produce/manage numerous keys. For security reasons, a given key ought to be changed as often as possible, even in each session.
- **Incompleteness:** It is difficult to implement a portion of the security services referenced previously. Specifically, authentication and non-repudiation can't be completely executed by just utilizing secret-key cryptography.

10.2 Hash Functions:

A Hash function[54] H is a computationally efficient function that maps fixed binary chains of arbitrary length {0,1}* to bit sequences H(B) of fixed length. H(B) is the hash value or digest of B.

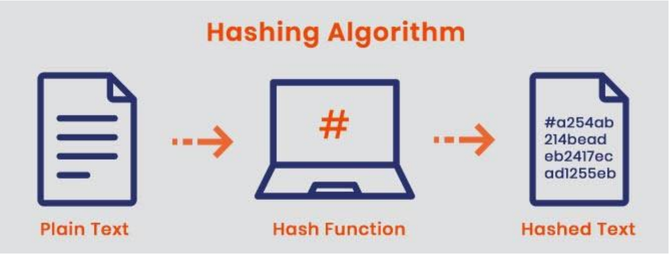


Figure 22:Hash Operation

In words, a hash work h maps bit-strings of self-assertive limited length to strings of fixed length, say n bits. MD5 and SHA-1 are two instances of hash capacities. MD5 produces 128-bits hash value while SHA-1 produces 160-bits hash value. Hash functions can be utilized for securing the client's secret key as portrayed in Fig. 22, shows the standard system utilized for achieving that objective. It is seen that the AES secret key is produced by methods for the hash value relating to the pass-phrase given by the users[35]. Another typical application of Hash functions is in the domain of pseudorandom sequences.

10.3 Symmetric Algorithm:

The symmetric algorithm is one in which the encryption and decryption key are the same. It is otherwise called private key cryptography. Symmetric key cipher is implemented as either block cipher or stream ciphers[36].

10.4 Asymmetric Algorithm:

The asymmetric cryptography algorithm is an algorithm wherein the key utilized in encryption is not the same as that of the key utilized decoding. It is otherwise called public-key cryptography. Whitfield Diffie and Martin Hellman, creators of the first published paper on public-key cryptography[36].

11.0 Bitcoin:

Bitcoin is a cryptographic currency dependent on open source software which was invented by an obscure individual or group of people utilizing the name Satoshi Nakamoto in 2009. It is a type of electric currency and the exchanges of bitcoins are checked by blockchain and the exchanges should be possible between client to client with no need of intermediaries[28]. Bitcoin's motivation of creation is to award for a procedure known as mining not just for that it tends to be traded for different monetary standards, products, and services.

References:

[1]. Mohd Zaid, Waqiyuddin Mohd Zulkifli , Evolution of Cryptography , pg no. 1-2, 17 January 2007.

[2]. David Kahn, The Code Breakers,Scribner, First Edition, 1967.

[3]. Evan Andrew, What was the Zimmermann Telegram?,History Stories, May 21,2014.

[4]. Choctaw_code_talkers, Wikipedia, World War I, DOA: January 2019.

[5]. https://www.tutorialspoint.com/cryptography/origin_of_cryptography.htm.

[6]. Tony M. Damico , A Brief History of Cryptography, vol. 1, No. 11, pg. 1, 2009.

[7]. Francisco Rodriguez-Henriquez, N.A. Saqib, Arturo Díaz Pérez, Cetin Kaya Koc, Cryptographic Algorithms on Reconfigurable Hardware, Spinger, 2007.

[8]. https://ssd.eff.org/en/module/deep-dive-end-end-encryption-how-do-public-key-encryption-systems-work.

[9]. Gurpreet Singh, Supriya, A Study of Encryption Algorithms (RSA, DES, 3DES, and AES) for Information Security, International Journal of Computer Applications (0975 – 8887) vol. 67, No.19, pg.1-4, April 2013.

[10]. Martin Schl¨affer, Cryptanalysis of MD4, Graz University of Technology, February 2006.

[11]. Junjun Gu et.al., Information Hiding for Trusted System Design, DAC Proceedings, ACM International Conference, 2009.

[12]. https://www.staff.unimainz.de/pommeren/Cryptology/Classic/2_Polyalph/Renaissance.html.

[13]. Wikipedia, Timeline of Cryptography, Semaphore Telegraph, DOA: January 2019.

[14]. Wikipedia, Timeline of Cryptography, Caeser cipher(100-1 A.D.), DOA: January 2019.

[15]. Wikipedia, Timeline of Cryptography, Morse Code, DOA: January 2019.

[16]. Wikipedia, Timeline of Cryptography, Stream_cipher, DOA: January 2019.

[17]. Wikipedia, Timeline of Cryptography,Lorenz Cipher, DOA: January 2019.

[18]. Wikipedia, Timeline of Cryptography, SIGABA, DOA: January 2019.

[19]. Marcus K. G. Adomey, Introduction to Cryptography, Africa CERT, pg. 4-5.

[20]. Asmi Bhattacharya, BASIC TERMS USED IN CRYPTOGRAPHY, www.acedemia.com.

[21]. https://www.ancient-origins.net/artifacts-ancient-writings/hidden-hieroglyphs-ancient-egyptian-lost-language-006653.

[22]. Anjney Pandey, Subhranil Som, Applications and usage of visual cryptography, IEEE, September 2016.

[23]. The Editors of Encyclopaedia Britannica, Hieroglyph, Encyclopaedia Britannica.

[24]. Nicholas G. McDonald, Past Present and Future Methods of Cryptography and Data Encryption, https://my.eng.utah.edu/~nmcdonal/Tutorials/EncryptionResearchReview.pdf, DOA: 07/01/2020.
[25]. Wikipedia, Timeline of Cryptography, Scytale, DOA: September 2018.
[26]. Wikipedia, Timeline of Cryptography, RSA (Cryptosystem), DOA: September 2018.
[27]. Wikipedia, Visual Cryptography, DOA: September 2018.
[28]. Wikipedia, bitcoin, DOA: September 2018.
[29]. Wikipedia, DeCSS, DOA: September 2018.
[30]. Wikipedia,Semaphore_telegraph,DOA: September 2018.
[31]. Wikipedia, Enigma machine, DOA: September2018.
[32]. Wikipedia, Cryptography, DOA: September 2018.
[33]. Sanjay Kumar Pal, 21st-century information technology revolution, ACMUbiquity, vol. June 2008.
[34]. Sanjay Kumar Pal et. al., Cryptography Based on RGB Color Channels Using ANNs, International Journal of Computer Network and Information Security, vol. 5, pg. 60-69, May 2018.
[35]. Sanjay Kumar Pal et. al., An Encryption Technique based upon Encoded Multiplier with Controlled Generation of Random Numbers, International Journal of Computer Network and Information Security, vol. 10, pg. 50-57,September 2015.
[36]. Sanjay Kumar Pal et. al., Application of Cosmos's law of Merge and Split for Data Encryption, International Journal of Computer Network and Information Security, vol. 5, pg. 11-20, May 2017.
[37]. https://www.britannica.com/topic/hieroglyph, DOA: September 2018.
[38]. https://pubweb.eng.utah.edu/~nmcdonal/Tutorials/EncryptionResearchReview.pdf, DOA: September 2018.
[39]. https://en.wikipedia.org/wiki/Scytale#/media/File:Skytale.png,DOA: September2018.
[40]. https://en.wikipedia.org/wiki/Caesar_cipher,DOA: September 2018.
[41]. https://www.staff.unimainz.de/pommeren/Cryptology/Classic/2_Polyalph/Renaissance.html
[42]. https://pubweb.eng.utah.edu/~nmcdonal/Tutorials/EncryptionResearchReview.pdf.
[43]. https://en.wikipedia.org/wiki/Semaphore_telegraph#/media/File:OptischerTelegraf.jpg, DOA: September 2018.
[44]. https://en.wikipedia.org/wiki/Jefferson_disk#/media/File:Jefferson%27s_disk_cipher.jpg,DOA: September 2018.
[45]. https://en.wikipedia.org/wiki/Morse_code#/media/File:International_Morse_Code.svg, DOA: September2018.
[46]. https://en.wikipedia.org/wiki/Zimmermann_Telegram#/media/File:Zimmermann_Telegram_as_Received_by_the_German_Ambassador_to_Mexico_-_NARA_-_302025.jpg.
[47]. https://en.wikipedia.org/wiki/Enigma_machine#/media/File:Enigma_(crittografia)_-_Museo_scienza_e_tecnologia_Milano.jpg ,DOA: September 2018.
[48]. https://billtuttememorial.org.uk/codebreaking/the-lorenz/, DOA: September 2018.
[49]. https://en.wikipedia.org/wiki/SIGABA,DOA: September 2018.
[50]. http://users.telenet.be/d.rijmenants/en/visualcrypto.htm, DOA: October 2018.
[51]. https://en.wikipedia.org/wiki/DeCSS#/media/File:DeCSS.svg, DOA: October 2018.
[52]. https://www.archives.gov/education/lessons/zimmermann,DOA: September 2018.
[53]. https://www.archives.gov/education/lessons/zimmermann,DOA: September 2018.
[54].https://www.archives.gov/education/lessons/zimmermann,DOA: September 2018.