Applications of Information Cryptography in Its Various Stages of Evolution, from Antiquity to the Modern Era

Nnaemeka Uchenna Ezeonyi, Obikwelu Raphael Okonkwo & Obinna Arthur Enweka

Abstract

Communication is a daily activity. Information needs to be move from a sender to a receiver, for a communication to hold. However, there are information or messages that should be kept secret and does not require knowledge of a third party. Such messages are encrypted or coded into a cipher text, so as to make no meaning to a third party who may eventually intercept it. This coding of information is called Encryption, while Decryption is the reverse of encryption. Thus, Cryptography is the process of encryption of plain texts and decryption of cipher texts. Cryptography began in early civilizations of Hebrew, Egypt, and Rome with the Atbash, Hieroglyph and Ceaser's Ciphers respectively. This period is regarded as the "Antiquity". Cryptography later evolved into Classic Cryptography, in the Middle Ages, where the "Key Model" and "Cryptanalysis" or code-breaking were introduced. Furthermore, Cryptography evolved to "Field Ciphers" and "Tele-Printer Ciphers" during the World War I. Moreover, the World War II saw the evolution of cryptography into various "Cipher Machines". In modern times, cryptography evolved into sophisticated mathematical equations called "Algorithms", for encrypting and decrypting messages. At these various evolution stages, cryptography is seen to be applied in civil communications, wars, cryptanalysis and e-commerce.

Keywords: cryptography, cryptanalysis, ciphers, encryption, decryption, data.

1.0 Introduction

Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it (Richards, 2021).Cryptography is one of the techniques used to ensure secure transmission of information via a channel between a pair of communicators. This prevents third parties from being acquainted with the data in transit (Peralta et al,

2014).Cryptography is a Greek word that means ‘secret writing’. Cryptography is the science of both encryption and decryption. Encryption is the process of encoding a message in such a way as to hide its contents. A plain or normal text sent over the network is converted into cipher text so that the information can only be used by the sender and the receiver (Krishna and Manikandan, 2020). The reverse process of encryption is called Decryption. It is the process of converting Cipher Text into Plain Text. Cryptographers use the decryption algorithms at the receiver side to obtain the original message from non-readable message i.e. Cipher Text (Naser, 2021). However, from ancient times till this modern times, several cryptographic techniques have been invented. This study presents cryptography in different era and are treated in the following order:

- Cryptography in the Antiquity
- Cryptography in the Middle Ages (*Classical Cryptography*)
- Cryptography in the World War I
- Cryptography in the World War II
- Modern Cryptography

2.0 Main Body

2.1 Cryptography in Antiquity

Antiquity is any period before the European Middle Ages (5th to 15th centuries) but still within the history of Western civilization ("Antiquity", 2023). According to Naser (2021), from the beginning of civilization when people started to live in different tribes or groups, each of them got the idea to be more powerful than others and to rule other tribes. So they feel for a secure and secret communication and thus how the process of primary cryptography was introduced. Hebrew scholars made use of simple mono-alphabetic substitution ciphers (such as the Atbash cipher) beginning perhaps around 600 to 500 BC ("Antiquity", 2023). Early civilizations in Egypt, Greece, and Rome adopted encryption for communication. Nearly 1900 B.C. (2000 B.C.), in ancient Egypt, a non-standard encryption was utilized on hidden “hieroglyphics” engraved on stone—the earliest known instance of cryptography—to conceal the meanings from those who did not know them, and for the amusement (Naser, 2021).By later periods of antiquity, cryptography was widely used to protect important military information, a purpose that it still serves to this day. A prominent example of Roman cryptography, known

as the Caesar cipher, involved shifting the letters of an encrypted message by a certain number of places down the Latin alphabet. Knowing this system and the number of places to shift the letters, a recipient could successfully decode the otherwise illegible message.

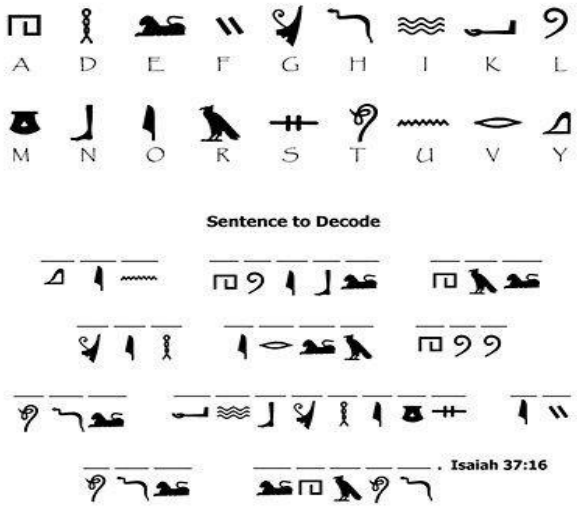

Figure 1: Hieroglyph (First techniques of Cryptography) (Hashmi and Choubey, 2018).

Below is a summary of the cryptographic techniques in Antiquity.

Period	**Cryptographic Techniques**		
Antiquity (5th to 15th Century)	(1). Atbash Cipher • 600 – 500 BC • By Ancient Hebrew • Used in Civil Communications • Mono-Alphabetic Substitution Technique	(2). Hieroglyph • 300 BC • By Ancient Egypt • Used in Wars and in Civil Communications • Pictorial Writing Technique	(3). Caesar Cipher • 100 BC • By Julius Caesar and Roman Armies • Used in War • Mono-Alphabetic Shift Technique

2.2 Cryptography in the Middle Ages (Classic Cryptography)

According to Hashmi and Choubey (2018), around 500 – 600 BC, Cryptography became popular, so encryption followed these methods:

- Substitution
- Transposition
- Codes

- Additionally, Cryptanalysis began in the Medieval ("History of Cryptography", 2023)

2.2.1 Substitution cryptographic method

This was the first cipher method which makes use of key model. Therefore, it can be called a 'Substitution Cipher'. Key means replacing alphabet to other alphabet for some secret rule. This rule becomes called a key (Abbasi and Singh, 2021).

There are Two (2) applications of substitution method.

i. Mono-Alphabetic Cipher

According to Aung et al. (2019), in Mono-Alphabetic substitution, a character (or a symbol) in the plain text is always changed to the same character (or a symbol) in the cipher text regardless of its position in the text (Aung et al., 2019).Examples are: Additive cipher, Shift cipher, Caesar cipher, Multiplicative cipher, Affine cipher, etc.

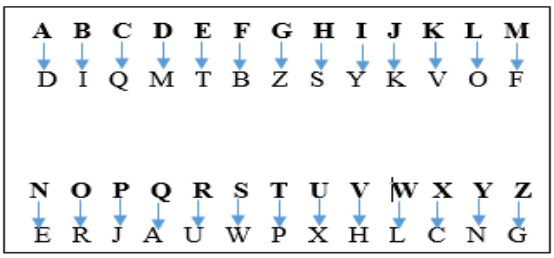

Figure 2: A Mono-Alphabetic Substitution Cipher (Hashmi and Choubey, 2018)

ii. Poly-Alphabetic Cipher

In Poly-Alphabetic substitution, each occurrence of a character may have a different substitute. (Aung et al., 2019). Examples of Poly-Alphabetic ciphers are: Vigenère cipher, Autokey cipher, Playfair cipher, Beaufort cipher, Running key cipher, Porta cipher, Hill cipher, One-Time pad, Rotor cipher, etc.

2.2.2 Transposition cryptographic method

According to Twum et al (2019), transposition ciphers shuffles characters around, instead of substituting them with other characters, as in the Substitution Method treated earlier. A transposition cipher is one which rearranges the order of the letters in the cipher text (encoded text), according to some predetermined method, without making any substitutions (Nrich, 2018).

E	N	E	M	Y	T	A
N	K	S	A	P	P	R
O	A	C	H	I	N	G
H	I	L	L	E	I	G
H	T	S	I	X	T	H
R	E	E	S	T	O	P

Plain Text: ENEMY TANKS APPROACHING HILL EIGHT SIX THREE STOP

Cipher Text: ENOHH RNKAI TEESC LSEMA HLISY PIEXT TPNIT OARGG HPXXX

Figure 3: A Simple Columnar Transposition Cipher (UMich, 2018).

2.2.3 Codebook cryptographic method

Codebook makes use of codes to replace a word or a phrase. Using Code, it was a good way to obfuscate meaning if the message is small and the codebooks are safe (Hashmi and Choubey, 2018).

plaintext	attack	to	taj	on	five	dec	eighteen
symbol	&	%	@	!	<	#	?

Figure 4: A Codebook Cipher Method (Hashmi and Choubey, 2018)

2.2.4 Cryptanalysis

Frequency Analysis technique was designed by Al-Kindi, an Arab mathematician, for breaking mono-alphabetic substitution ciphers. This was around AD 800, in the medieval ("History of Cryptography", 2023). Cryptanalysis means trying to break any security system (or cipher) by using unauthorized ways to access the information in that system. Thus, cryptanalysis works against cryptography. The cryptanalyst tries to find any weakness in the cryptographic system to get either the source of information (plaintext) or the key used in the encryption algorithm (Al-Janabi, Al-Khateeb and Abd, 2017). The objective of cryptanalyst is to be able to decrypt cipher text (Tiwari, Nandi and Mishra, 2013). In the modern era, among several instances, Brute-force key-space search has broken some real-world ciphers and applications, including single-DES, 40-bit "export-strength" cryptography, and the DVD Content Scrambling System. In 2008, researchers conducted a proof-of-concept break of SSL using weaknesses in the MD5 hash function and certificate

issuer practices that made it possible to exploit collision attacks on hash functions ("Cryptanalysis", 2023). In World War II, the Allies benefitted enormously from their joint success cryptanalysis of the German ciphers – including the Enigma machine and the Lorenz cipher – and Japanese ciphers, particularly 'Purple' and JN-25. In World War II, the Enigma cipher system was broken by Polish and British cryptographers. ("Cryptanalysis", 2023). Below is a summary of cryptographies used in the medieval period.

Period	**Cryptographic Techniques**			
Medieval (500 – 1500 CE)	(1). Substitution • Makes use of Ciphers • Substitutes alphabets with another • Used in Civil Communications	(2). Transposition • Makes use of Ciphers • shuffles characters around • Used in Civil Communications	(3). Codebook • Makes use of Codes to replace words or phrases • Used in Civil Communications where the message is small and codebooks are safe • Used in Wars	(4). Cryptanalysis • The cryptanalyst tries to find any weakness in the cryptographic system in order to break the code. Thus, cryptanalysis works against cryptography.

2.3 Cryptography in the World War 1

According to Cthaeh (2021), Radio was invented at the very end of the 18th century and World War I and became the first big war in which it was used. Naturally, making communications more effective also increased communication traffic by several orders of magnitude.World War I has a timeline from 28th July, 1914 to 11th November, 1918 (Ray, 2018). According to Cthaeh (2021), World War I is the second largest military conflict in history, surpassed only by World War II. The war was fought between two camps — the Central Powers and the Allied Powers — and lasted until late 1918. The main participants on the side of the Central Powers were Germany, Austria-Hungary, the Ottoman Empire, and Bulgaria. On the side of the Allied Powers were France, Britain, Russia, and Italy. Many other countries joined the conflict at different stages (including the United States on the side of the Allied Powers). The invention of the electric telegraph increased the traffic of messages dramatically. Messages could now travel through electric wires close to the speed of light.

2.3.1 Standard codes used in World War I

Cthaeh (2021) stated that the most common use of codes was for naval, diplomatic, and strategic communication. In general, using codes is more cumbersome compared to ciphers, since the encoding/decoding process is significantly slower and the secure distribution of codebooks is always a challenging task, especially when the communicating parties are constantly on the move. On the other hand, these codes were considered far more secure than ciphers. That's why they were preferred for communication that required absolute secrecy.

Trench Codes: These were less sophisticated codes with a much smaller vocabulary of up to only a few thousand words, used by armies inside trenches. They were less secure but easier to distribute. The lower security wasn't necessarily a serious issue. Even if the enemy managed to break the code for a particular message, it wouldn't matter too much unless they break it fast enough. The situation on the battlefield is changing quickly and old information becomes useless very fast (Cthaeh, 2021).

2.3.2 Field ciphers used in World War I

i. Playfair (British): The Playfair cipher system was widely used by American army and English Army during the World War I (Shang & Lu, 2012).The British used it for tactical communication. Later on, the Americans picked it up too when they joined the war (Cthaeh, 2021).

ii. Interrupted Columnar Transposition (French): The French used the interrupted columnar transposition cipher for very similar purposes to the British's use of the Playfair cipher (tactical communication on the battlefield) (Cthaeh, 2021).

iii. Turning Grilles Cipher (German): This is a pure transposition cipher that uses a square made up of smaller squares. Crucially, there were holes at the positions of a quarter of the smaller squares. The Germans used squares of different sizes, depending on the length of the message they wanted to send (like 7×7 or 10×10), always removing a quarter of the small squares (Cthaeh, 2021).

iv. ADFGX and ADFGVX cipher (German): The cipher's name initially was **ADFGX** and shortly after it became **ADFGVX**, after a small modification. However, the ADFGVX modification doesn't change the nature of the cipher. Germany introduced it in early 1918 and used it for communications between divisions, corps, and army headquarters during the Spring Offensive I told you about earlier (Cthaeh, 2021).

v. Vigenere Cipher (Russia): Ernst Fetterlein was in the Tsarist Russian Ministry of Foreign Affairs from 1896 and solved (among others) German, Austrian and British codes. He became chief cryptographer with the rank of admiral. The Russians used an overcomplicated version of the Vigenère Cipher. It was broken within three days by Austro-Hungarian cryptanalyst Hermann Pokorny (Cthaeh, 2021).

2.3.3 Tele-printer ciphers used in World War I

In 1917, Gilbert Vernam proposed a tele-printer cipher in which a previously prepared key, kept on paper tape, is combined character by character with the plaintext message to produce the cypher text. This led to the development of electromechanical devices as cipher machines, and to the only unbreakable cipher, the One-Time pad (Rijmenants, 2022).

One-Time Pad

To perform one-time pad encryption, we need a key, called one-time pad. A one-time pad can be a single sheet, a booklet or a strip or roll of paper tape that contains series of truly random digits. A one-time pad set consists of two identical one-time pads, one pad called OUT and one called IN. To establish one-way communications, you only need one OUT pad for the sender and an identical copy called IN pad for the receiver. To communicate in both ways, you need two different one-time pad sets: person A has an OUT pad of which person B has the IN copy, and person B has another OUT pad of which person A has the IN copy (Rijmenants, 2022). Below is a summary of cryptography used in the World War 1

Periods	**Cryptographic Techniques**		
World War 1 (1914 - 1918)	(1). Codebooks • Makes use of Codes to replace words or phrases • Used in Civil Communications where the message is small and codebooks are safe • Used in World War 1 (Codebook with super-encryption). • Example: **Trench Codes.**	(2). Field Ciphers i. PlayFair Cipher (British) ii. Interrupted Columnar Transposition (French) iii. Turning Grilles Cipher (Germany) iv. ADFGX and ADFGVX cipher (Germany) v. Vigenere Cipher (Russia)	(3). Tele-Printer Ciphers • This is a technique, in which a previously prepared key, kept on paper tape, is combined character by character with the plaintext message to produce the cypher text. • Example: One Time Pad Cipher

2.4 Cryptography in the World War II

By World War II, mechanical and electromechanical cipher machines were in wide use ("History of cryptography", 2023). The World War II has a timeline from 1939 to 1945. The principal belligerents were the Axis powers—Germany, Italy, and Japan —and the Allies—France, Great Britain, the United States, the Soviet Union, and, to a lesser extent, China (Hughes and Royde-Smith, 2023).

In the 1920s, various mechanical encryption deviceswere invented to automate the process of encryption. Most were based on the concept of a rotor, a mechanical wheel wired to perform a general substitution (Sokouti, Sokouti and Pashazadeh, 2009).

2.4.1 Cipher machines used in World War II

Enigma (Germany): As complicated as the Enigma was, it was broken during World War II. First, a team of Polish cryptographers broke the German Enigma and explained their attack to the British. The Germans modified their Enigma as the war progressed, and the British continued to cryptanalyze the new versions (Sokouti, Sokouti and Pashazadeh, 2009).

Fig 5: The German Enigma ("History of cryptography", 2023)

Purple (Japan): In the early 1930s, the Japanese government purchased the commercial version of the Enigma machine from the German government in order to build an enhanced version of it. This cryptographic machine was named ''Red" by the US government. Soon after the ''Red" cipher was broken by the U.S.A, the Japanese government created a more evolved and secure cipher known as ''97-shiki O-bun In-ji-ki" or ''97 Alphabetical Typewriter", named for its creation on the Japanese year 2597 in 1937. The US later named it as Purple. Unlike the Enigma machine, which used the blinking lights to represent the message, Purple used an electric typewriter, which could

write the message on paper. This was easy to use than the Enigma machine. However, it was heavy and tedious to carry in combat areas. It was a complex machine used to encrypt data not only in the 1930s, but even today. It falls under the category of homophonic substitution ciphers, where a single plaintext letter can be replaced by any of the different cipher text letters. (Shikhare, 2015).

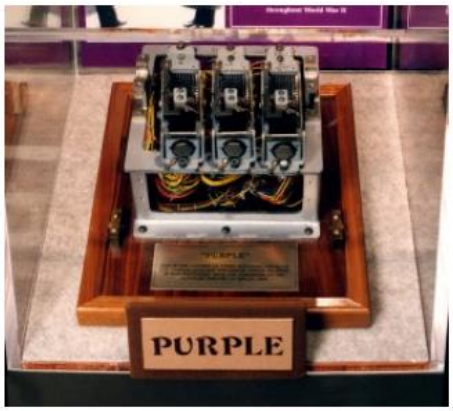

Fig 6: The Japanese 'Purple'(Shikhare, 2015)

Typex (Britain): After the World War I, the British government in 1926, established the Inter-Departmental Cipher Committee to explore possible cipher machines to replace their current book cipher systems. In 1935, the Committee decided upon "Enigma type cipher machines improved through the use of 'Type X' attachments" or Typex. The Typex machine, developed by Wing Commander O.G.W. Lywood, was such a close relative of the Enigma machine that the British use Typex machines in place of Enigma when trying to decipher Enigma messages. When German soldiers recovered a Typex machine sans rotors, they successfully converted it into an Enigma machine. This similarity discouraged German cryptanalysts from attempting to cryptanalyze Typex enciphered messages because they believed Enigma to be unbreakable (Chang, 2012).

Fig 7: The British 'Typex' (Chang, 2012).

Sigaba (USA): SIGABA is a cipher machine used during World War II until the 1950s. It takes a shot at the electromechanical arrangement of rotors (Pal, Datta and Karmakar, 2020). In the 1930s, the U.S. Army cryptologist William Friedman and his assistant Frank Rowlett drew on this simple precept to conceive a cipher machine that was easy to use, simple to rekey, and ostensibly impossible to break. To the Army it was known as SIGABA, to the Navy, ECM (Electric Cipher Machine) II. Not only was SIGABA the most secure cipher machine of World War II, but it went on to provide yeoman service for decades thereafter (Mucklow, 2015)

Fig 8: The USA 'SIGABA' (Mucklow, 2015)

Below is a summary of cryptography used in the World War II.

Period	**Cryptographic Techniques**	
World War II (In the 1920's)	(1). Codebooks • Used in World War 2 (Eg. The Japanese JN-25 Code)	(1). Cipher Machines Mechanical encryption devices that were invented to automate the process of encryption. Most were based on the concept of a rotor, a mechanical wheel wired to perform a general substitution. Examples: i. Enigma (Germany) ii. Purple (Japan) iii. Typex (Britain) iv. Sigaba (USA)

2.5 Modern Cryptography

Around 1990, the use of the Internet for commercial purposes, the introduction of online commercial transactions and as wireless networks became more common among households, the need for encryption grew, as a level of security was needed in these everyday situations ("History of Cryptography", 2023). Adomey (2020) explained three (3) types of Cryptography:

i. Secret (Symmetric) Key Cryptography

ii. Public (Asymmetric) Key Cryptography

iii. Hash Functions

iv. Hybrid Cryptography (additional)

2.5.1 Secret (Symmetric) key cryptography

The Symmetric Key Cryptography is also known as Secret Key Cryptography or Conventional Cryptography. The Symmetric Key Cryptography is an encryption system in which the sender and receiver of a message share a single, common key used to encrypt and decrypt the message. It uses an algorithm called Secret Key Algorithm or Symmetric Algorithm (Adomey, 2020).

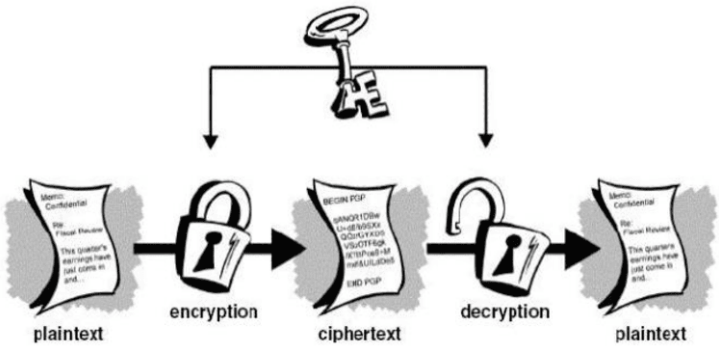

Figure 9: Symmetric Key Cryptography (Adomey, 2020)

Some examples of popular Symmetric Key Cryptography are: DES – Data Encryption Standard, Triple-DES, AES – Advanced Encryption System, Rivest Cipher 4 (RC4).

2.5.2 Public (asymmetric) key cryptography

According to Adomey (2020), Asymmetric cryptography, also known as Public-key cryptography, refers to a cryptographic algorithm which

requires two separate keys, one of which is private and one of which is public. The public key encrypts the message while the private key decrypts the encrypted message. Public Key Cryptography is a very advanced form of cryptography. Officially, Whitfield Diffie and Martin Hellman invented it in 1975. The British Clifford Cocks of Communications-Electronics Security Group (CESG) of (Government Communications Headquarters - GCHQ) first discovered the basic technique of public key cryptography in 1973 but this was a secret until 1997. The figure below depicts a public key cryptography.

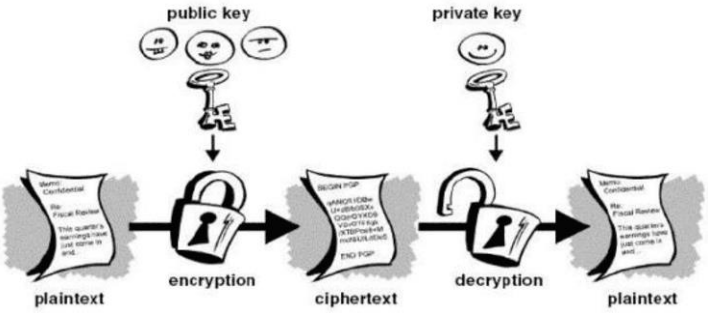

Figure 10: Public (Asymmetric) Key Cryptography (Adomey, 2020)

Some examples of asymmetric cryptography are: Rivest-Shamir-Adleman (RSA) Algorithm, Digital Signature Standard, EIGamal, etc.

2.5.3 Hash functions

According to Kundu and Dutta (2020), hash functions refer to a function that compresses a string of arbitrary input to a string of fixed length. In other words, we get a fixed-length message digest out of a variable-length message. Compared to the message the digest is normally much smaller. The main purpose of hashing is related with message security like protecting message integrity, authenticity, etc. Wahome (2021) further explained that using hash functions for cryptography refers to cryptographic hash function. He continued that all cryptographic hash functions are hash functions, but not all hash functions are cryptographic hash functions. Mathematically, Wahome classified cryptographic hash functions into two classes:

- Unkeyed hash functions also known Manipulation Detection Code (MDC) or Message Authentication Code (MAC) with a single parameter, an input message.
- Keyed hash functions with two distinct input, an input message and a secret key.

Wahome (2021) also listed the examples of cryptographic hash functions

as follows:

- The Secured Hash Algorithm (SHA) family - They are six hash functions: SHA -0, SHA – 1, SHA – 224, SHA – 256, SHA – 384 and SHA – 512. The first four operate on 512-bit message blocks divided into 32-bit words and the last two on 1024-bit blocks divided into 64-bit words. Bitcoin, the original and largest cryptocurrency (at the time of writing), uses the SHA-256 hash function.

- **The MD (Message Digest)** family — comprises of MD2, MD4, MD5 and MD6 authored by Ronald Rivest for RSA security and was adopted as the Internet Standard RFC 1321.

- **RIPEMD (RACE Integrity Primitives Evaluation Message Digest)** — a family of cryptographic hash functions based upon the design principles used in MD4 developed by Hans Dobbertin, Antoon Bosselaers, and Bart Preneel at the COSIC research group at the Katholieke Universiteit Leuven. RIPEMD-160 produces a hash digest of 160 bits (20 bytes).

- **Whirlpool** — designed by Vincent Rijmen and Paulo S. L. M. Barreto, this hash function based on a substantially modified version of the Advanced Encryption Standard (AES). Whirlpool produces a hash digest of 512 bits (64 bytes).

- **BLAKE** — a hash function submitted to the NIST hash function competition by Jean-Philippe Aumasson, Luca Henzen, Willi Meier, and Raphael C.-W. Phan. It is based on Dan Bernstein's ChaCha stream cipher, but a permuted copy of the input block, XORed with round constants, is added before each ChaCha round.

- **Curl-P** — a hash function formerly used in IOTA Signature Scheme (ISS). IOTA is a cryptocurrency designed for use with the Internet of Things (IoT) and automotive ecosystems. ISS is based on Winternitz One-Time Signatures but unlike traditional Winternitz, in IOTA users sign the hash of a message. Thus, the security of ISS relies on its cryptographic hash function, which was Curl-P-27.

2.5.4 Hybrid cryptographic systems

Hybrid cryptography means combining two or more cryptosystems. There are benefits and limitations in both symmetric and asymmetric

ciphers. Symmetric ciphers are fast but suffer key exchanging. Asymmetric ciphers solve the key exchange problem, in other words secure, but slow. Practically, hybrid cryptography, which is an integration of symmetric and asymmetric ciphers, makes use of the efficiency of symmetric ciphers and the simplicity and security of asymmetric ciphers (Murad and Rahouma, 2021b).

2.5.4.1 Approaches to hybrid cryptography

In this study, three (3) approaches to hybrid cryptography were studied:

Double Encryption (of Symmetric or Asymmetric)

The first approach, according Murad and Rahouma (2021a), involves performing two layers of symmetric or asymmetric encryption. Here, data is double encrypted by applying two consecutive, either symmetric or asymmetric ciphers in a row. See figure below.

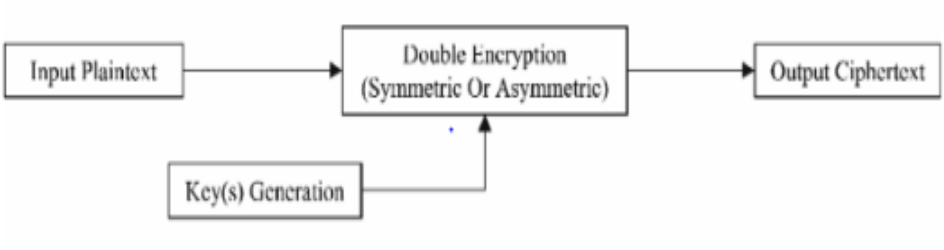

Figure 11: Hybrid scheme uses double encryption of either symmetric ciphers or asymmetric ciphers for data encryption (Murad and Rahouma, 2021a)

Symmetric / Asymmetric Hybrid Cryptography

As shown in the next figure below, this approach utilizes a symmetric algorithm to encrypt the data and applies an asymmetric algorithm to encrypt the secret key. See figure below.

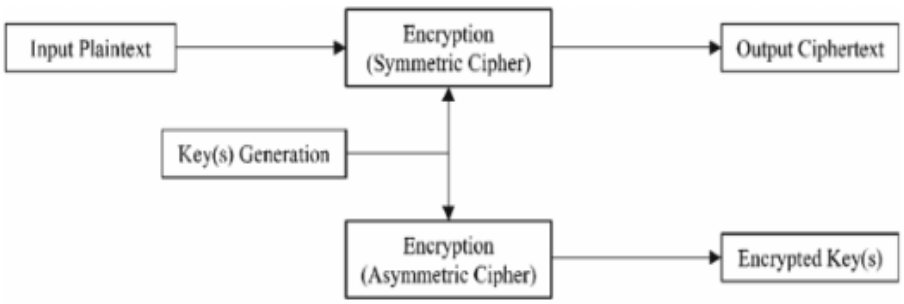

Figure 12: Hybrid scheme uses symmetric ciphers for data encryption and asymmetric ciphers for key encryption (Murad and Rahouma, 2021a)

Cryptography with other Supportive Methods (i.e. with other technologies)

To further strengthen cryptography, researchers have presented schemes where supportive methods were used to improve cryptography security level. Examples of such supportive methods are:

- Hybrid cryptography and steganography method to embed encrypted text message within image (Jassim, et al., 2019)
- A hybrid scheme of cryptography and watermarking (Kaur and Kaur, 2016)
- A hybrid cryptographic technique using RSA algorithm and scheduling concepts (Shankar and Akshaya, 2014)

These supportive methods are applied to increase the strength of a symmetric / asymmetric hybrid algorithm.

Below is a summary of cryptography used in the modern era.

Period	**Cryptographic Techniques**			
Modern Era	(1). Symmetric (Secret key) Cryptography Sender and receiver of a message share a single, common key, used to encrypt and decrypt the message. **Examples**: i). Data Encryption Standard (DES) ii). Triple-DES iii). Advanced Encryption System (AES) iv). Rivest Cipher 4 (RC4) Etc.	(2). Asymmetric (Public key) Cryptography This requires two separate keys, one of which is private and one of which is public. The public key encrypts the message while the private key decrypts the encrypted message. **Examples**: i). Rivest-Shamir-AdlemanAlgorithm(RSA) ii). Digital Signature Standard iii). EIGamal Etc.	(3). Hash Functions Here, we get a fixed-length message digest out of a variable-length message. **Examples**: i). Secured Hash Algorithm (SHA) family ii). MD (Message Digest) family iii). RIPEMD family iv). Whirlpool v). Blake vi). Curl-P	(4). Hybrid Cryptography Hybrid cryptography means combining two or more cryptosystems. **Approaches**: 1). Double Encryption (AES + AES) 2). Symmetric + Asymmetric (AES + RSA) 3). Cryptography + Supportive Methods. Eg: - (RSA + Scheduling Concepts)

3.0 Conclusion

Based on the above reviews, cryptography has evolved in so many ways and is still evolving. It has been found to be applied in the following ways:

i. Civil Communication

Cryptography is applied in encrypting messages in civil communications or messages between two regular individuals or organizations. Starting from antiquity, through the medieval, and through the world wars, and in the modern era, messages can be encrypted to ensure confidentiality. Emails are usually encrypted in order to keep them confidential. As messages travel through communication links, both wired and wireless, they are often encrypted.

ii. Cryptanalysis

Cryptanalysis is as an application of cryptography, though as a reverse process. Cryptanalysis began in the Medieval period. This is because classical cryptography began in this era, with the introduction of keys-based cryptography or ciphers. The medieval period cryptographic methods and those used in the world wars were at a point in time broken. In this modern era, cryptographic systems are not easily broken, because, they cannot be solved by hand. However, the One-Time-Pad is a Tele-Printer Cipher which has never been broken.

iii. Wars

In antiquity, Hieroglyphs were used to encrypt messages between soldiers. Cryptography in wars was mostly applied in the World War I and in the World War II. Cryptography is very essential during wars since each army group needs to frequently send messages to their colleagues in case of a need of unfavorable circumstances like need for back-up, need for a retreat, need for change of plans or change of direction, need for supply of more ammunitions. The message must be confidential, otherwise the enemy camp will know their plans and move ahead of them.

iv. E-Commerce

Cryptography is very important and is carefully applied for commercial purposes. Encryption keeps your data secure when you're shopping or banking online. It scrambles data like your credit card details and home address to ensure hackers can't misuse this information. Cryptography in e-commerce ensures data privacy.

References

Abbasi, F. and Singh, P. (2021). Cryptography: Security and integrity of data management. *Journal of Management and Service Science,*1(2), 1 – 9.

Adomey, M.K.G. (2020). *Introduction to Cryptography* [PowerPoint Slides]. Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/ Documents/01-Introduction%20to%20Cryptography.pdf, on 30 August 2021.

Al-Janabi, S.T., Al-Khateeb, B. and Abd, A.J. (2017). Intelligent techniques in cryptanalysis: Review and future directions. *UHD Journal of Science and Technology*, 1(1), 1 – 10.

Antiquity. (2023, April 6). In *Wikipedia*. https://en.wikipedia.org/wiki/ Antiquity

Aung, T. M., Naing, H. H. and Hla, N. N. (2019). A complex transformation of mono-alphabetic cipher to poly-alphabetic cipher: (Vigenère-Affine Cipher). *International Journal of Machine Language and Computing*, 9 (3), 296 – 303.

Chang, K. (2012). *Cryptanalysis of Typex* [Master's thesis, San Jose State University]. https://www.cryptomuseum.com/crypto/uk/typex/files/kelly.pdf

Cthaeh (2021, May 10). *Cryptography During World War I*. Retrieved May 24, 2023, from https://www.probabilisticworld.com/ cryptography-during-world-war-i/

Hashmi, A. and Choubey, R. (2018). Cryptographic Techniques in Information Security. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 3(1), 854 – 859.

History of cryptography. (2023, May 22). In *Wikipedia*. https://en. wikipedia.org/wiki/ History_of_cryptography

Hughes, T. A. and Royde-Smith, J. G. (2023, May 23). World War II. Encyclopedia Britannica. https://www.britannica.com/event/World-War-II

Jassim, K.N., Nsaif, A.K., Nseaf, A.K., Hazidar, A.H., Priambodo, B., Naf'an, E., Masril, M., Handriani, I. and Putra, Z.P. (2019). *Hybrid cryptography and steganography method to embed encrypted text message within image. In 2019 Journal of Physics: Conference Series, Volume 1339, International Conference Computer Science and Engineering*, 26 – 27th April 2019, Padang Indonesia: IOP Publishing, 1 – 9.

Kaur A. and Kaur R. (2016). A hybrid scheme for cryptography and watermarking. *International Journal of Advanced Research in Computer and Communication Engineering*, 5(7), 183 – 188.

Krishna, A and Manikadan, L.C. (2020). A study on cryptographic techniques. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 6(4), 321 – 327.

Kundu, R. and Dutta, A. (2020). Cryptographic hash functions and attacks – A detailed study. *International Journal of Advanced Research in Computer Science, 11(2)*, 37-44.

Mucklow, T. (2015). *The SIGABA / ECM II Cipher Machine: "A Beautiful Idea"*. USA: Center for Cryptologic History.

Murad, S.H., and Rahouma, K.H. (2021a). Hybrid Cryptographic Approach to Safeguard Cloud Computing Services: A Survey. In: Hassanien, AE., Chang, KC., Mincong, T. (Eds) *Advanced Machine Learning Technologies and Applications. AMLTA 2021.* (pp. 785 – 793). Springer.

Murad, S.H., and Rahouma, K.H. (2021b). Implementation and Performance Analysis of Hybrid Cryptographic Schemes applied in Cloud Computing Environment. *Procedia Computer Science*, 194(2021), 165 – 172.

Naser, S. M. (2021). Cryptography: From the ancient history to now, it's applications and a new complete numerical model. *International Journal of Mathematics and Statistics Studies*, *9*(3), 11-30.

Nrich (2018), *Transposition Cipher* [PowerPoint Slides]. Retrieved from https://nrich.maths.org/7940, on 25 August 2021.

Pal, S.K., Datta, B. and Karmakar, A. (2020). Cryptography and network security: a historical transformation. *SCHOLEDGE International Journal of Multidisciplinary and Allied Study*, 7(2), 30 – 44.

Peralta, D., Triguero, I., Sanchez-Reillo, R., Herrera, F. (2014). Fast fingerprint identification for large databases. *ACM Digital Library*, 47(2), 588 – 602.

Richards, K. (2021, September 1). *Cryptography*. Techtarget. Retrieved June 10, 2023, from https://www.techtarget.com/searchsecurity/definition/cryptography

Rijmenants, D. (2022). The complete guide to secure communications with the one-time pad cipher. *Cipher Machines and Cryptology*, 1 – 27.

Shang, Y., & Lu, L. (2012, July 18). *An extended algorithm based on playFair cipher* [Conference presentation]. Atlantis Press. https://www.atlantis-press.com/article/2979.pdf

Shankar M. and Akshaya P. (2014). Hybrid cryptographic technique using RSA algorithm and scheduling concepts. *International Journal of Network Security & Its Applications*, 6(6), 39-48.

Shikhare, A. (2015). *Cryptanalysis of the Purple Cipher using Random Restarts* (Publication No. 428) [Master's thesis, San Jose State University]. https://scholarworks.sjsu.edu/ etd_projects/428

Sokouti, M., Sokouti, B. and Pashazadeh, S. (2009). An approach in improving transposition cipher system. *Indian Journal of Science and Technology*, 2(8), 9 – 15.

Tiwari, G., Nandi, D. and Mishra, M. (2013). Cryptography and cryptanalysis: A Review. *International Journal of Engineering Research and Technology*, 2(10), 1898 – 1902.

Twum, F., Acquah, J.B. and William, M. (2019). A proposed enhanced transposition cipher algorithm based on Rubik's Cube transformations. *International Journal of Computer Applications*, 182 (35), 18 – 26.

Umich (2018). *Transposition Systems* [PowerPoint Slides]. Retrieved from http://websites.umich.edu/~umich/fm-34-40-2/ch11.pdf, on 25 August 2021.

Wahome M. (2021). Cryptographic Hash Functions. 1-9. Retrieved from https://www.researchgate.net/publication/351837904_Cryptographic_Hash_Functions, on 07 October, 2021.

Authors' Brief Data

Nnaemeka Uchenna Ezeonyi is System Analyst, University Library, Chukwuemeka Odumegwu Ojukwu Universty, Igbariam, Anambra State, Nigeria. *Email*: nu.ezeonyi@gmail.com.

Obikwelu Raphael Okonkwo is of the Department of Computer Science, Nnamdi Azikiwe University, Awka, Anambra State. *Email*: ro.okonkwo@unizik.edu.ng.

Obinna Arthur Enweka is affiliated to Department of Computer Science, Federal Cooperate College, Oji River, Enugu State, Nigeria. *Email*: enweka.arthur@gmail.com.