Sri Lanka Institute of Information Technology

B.Sc. (Hons) in Information Technology Specialized in Cyber Security

Introduction to Cyber Security-IE2022

Individual Assignment

IT23623972-T.M.G.H Thennakoon

Topic : CRYPTOGRAPHY

Table of Contents

Cryptography

Abstract

Cryptography is an important area in computer science and mathematics where information is encoded to ensure its privacy. As our world transitions to digital, cryptography ensures confidentiality, integrity, authentication and non-reputation. This paper is an extensive survey of the history of cryptography from the earliest times to the present and it also looks ahead to the future of cryptography, such as post-quantum cryptography homomorphic encryption and artificial intelligence inclusion. This survey aims to provide a broad overview of the everlasting importance of cryptography in secure computing by reviewing the fundamentals, latest developments and general trends.

1. Introduction to the Topic

Cryptography is an Ancient Greek derivation from the word kryptós for "hidden" or "secret," and graphein meaning "to write." Cryptography is the design, study, and evaluation of algorithms and protocols that offer secure communication. Cryptography in a broad context is the design, analysis, and evaluation of protocols that deny unauthorized access to sensitive information. Cryptography offers basic security properties such as confidentiality, integrity, authentication, and non-repudiation.

In essence, cryptography is the operation of transforming readable information, known as plaintext, into unreadable form known as ciphertext. Such transformation protects data from unauthorized viewing and can be reversed only through decryption using special keys or methods. Cryptography allows sensitive information to be transferred over insecure mediums without compromising security. A typical example used is Alice (sender) securely sending to Bob (receiver) with Eve (the attacker) attempting to intercept and read the message.

Cryptography is now an interdisciplinary field combining computer science, mathematics, information security, electrical engineering, digital signal processing, and physics. Cryptography used to be concerned primarily with message secrecy with ciphers. Its scope has hugely expanded in today's times. It now extends over a wide range of applications from authentication schemes (e.g., passwords and access control) through digital signatures to verify identity and integrity, cryptographic techniques for private computation used to protect data for privacy-preserving data processing, and cryptocurrencies which rely on cryptography for security as well as payment verification.

Overall, cryptography is a vital tool to ensure information security in an increasingly integrated digital age.

Cryptographic systems typically fall into three main categories:

1. **Symmetric Key Cryptography**: These systems both encrypt and decrypt using the same cryptographic key. AES (Advanced Encryption Standard) and the outdated DES (Data Encryption Standard) are examples of modern algorithms, whereas Caesar's and Vigenère are examples of primitive ciphers. Large datasets can be encrypted cheaply with symmetric algorithms, but safe key exchange is a trade-off.

2. **Asymmetric Key Cryptography**: Also known as public-key cryptography, these systems use different keys for encryption and decryption – a public key accessible to anyone and a private key known only to the owner. RSA and Diffie-Hellman key exchange are prominent examples that revolutionized cryptography by solving the key distribution problem.

3. **Hash Functions**: These are one-way functions that convert data of arbitrary size to a fixed-size output, producing a "digest" that serves as a digital fingerprint. Hash functions are essential for data integrity verification, password storage, and digital signatures.

The security of cryptographic methods is gauged by the extent to which they can withstand a range of attacks without compromising usability. Phil Zimmermann, the designer of Pretty Good Privacy (PGP), accurately summarized cryptography as "the art and science of keeping messages secure" both in a scientific and artistic sense. Because there has been progress in computing power and new forms of attacks are being conceptualized, cryptography also adapts to neutralize them.

Now, in this information age, one cannot emphasize enough the importance of cryptography. Cryptographic algorithms are depended upon by all secure web commerce, electronic commerce, digital signatures, and encrypted communications. As more and more society is reliant on digital infrastructure, defense against penetration by these mathematical systems becomes all the more critical to privacy protection, commerce facilitation, and sensitive communications safeguarding.

[1] [2] [3]

2. Evolution of Cryptography

- **Ancient Cryptography**
    - The earliest historical use of cryptography was in Egypt circa 1900 BC when non-standard hieroglyphics were written on the walls of monuments. Early uses were likely more for causing mystery or intrigue than for securing communications. Pragmatic purposes were discovered later in Mesopotamia in approximately 1500 BC where encrypted recipes on clay tablets for valuable pottery glazes were found.

    - Hebrew cryptographers devised simple monoalphabetic substitution ciphers such as the Atbash cipher around 600-500 BC, where each letter was replaced by its counterpart from the opposite end of the alphabet. While innovative, these techniques were not very secure since they were based on regular patterns and could be vulnerable to frequency analysis. [2]

    - The Scytale is an Ancient Cryptography method. It was used around 7th century BC by the Spartans (in Ancient Greece) for military secret communication. It belongs to the early history of cryptography, similar to the Egyptian hieroglyphics and the Atbash cipher you mentioned earlier. [2]

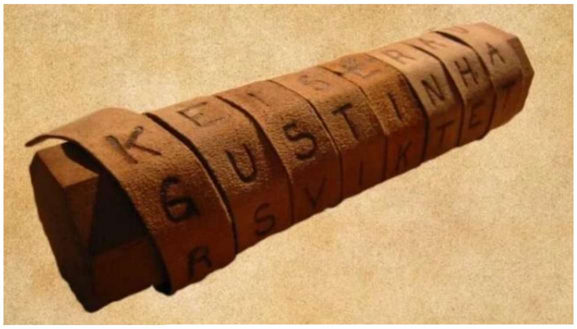


Figure 1:Scytale

- **Classical Cryptography**
  - The first famous cryptographic system is the Caesar cipher, which is named after Julius Caesar, who allegedly utilized it to scramble his private correspondence. Caesar, based on Suetonius' "Lives of the Caesars," used a straightforward substitution cipher where every letter was substituted with a letter three positions ahead in the alphabet. For example, 'A' would be substituted with 'D', 'B' with 'E', and so on. [4] [5]

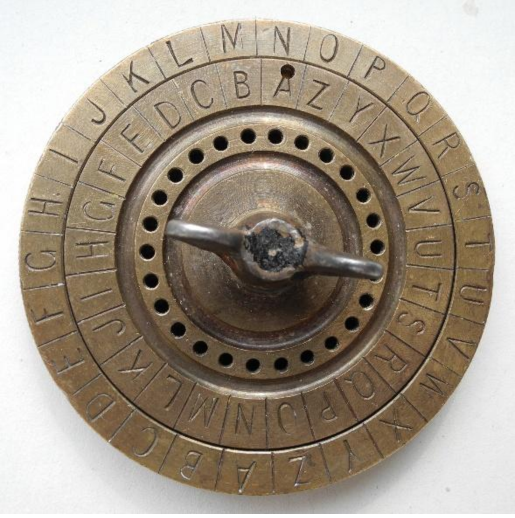
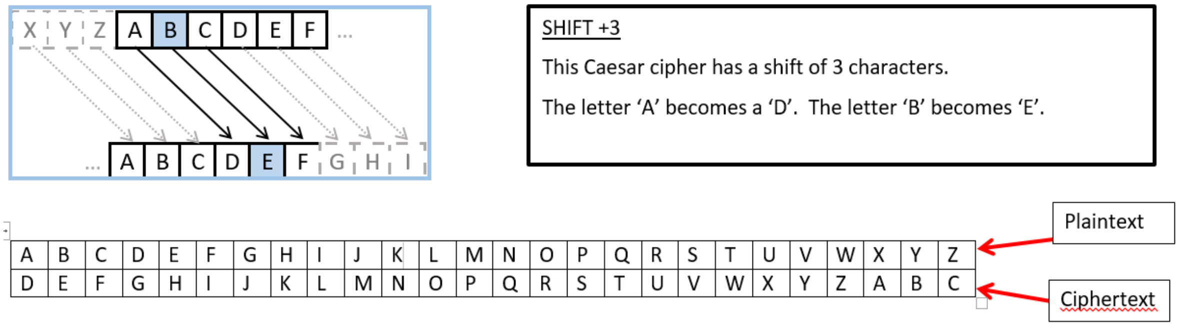


Figure 2:Caesar cipher

  - Caesar's replacement, Augustus, altered this plan by replacing each letter with the one that comes immediately after it. The simplicity of these ciphers rendered them appropriate for their time but also susceptible to cracking once the scheme was in place. A Caesar cipher with a shift of 13, known as ROT13, is still in use today in UNIX operating systems to scramble data against unauthorized reading – twice ROT13 restores the original. [4] [5]



SHIFT +3

This Caesar cipher has a shift of 3 characters.

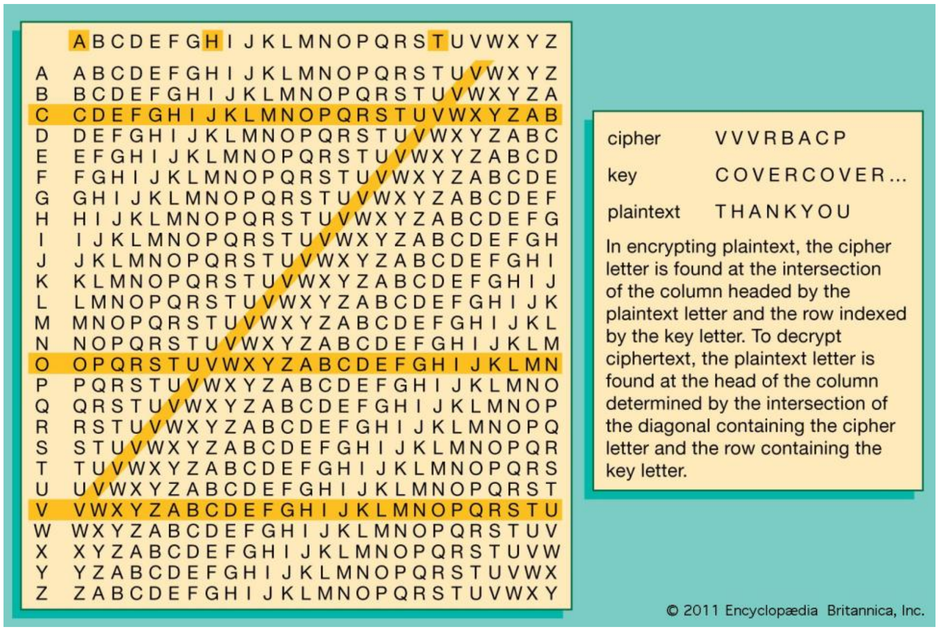
The letter 'A' becomes a 'D'. The letter 'B' becomes 'E'.

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	Plaintext
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	Ciphertext

Figure 3:A Caesar cipher with a shift of 3

  - A significant innovation in the 16th century was the Vigenère cipher, described by Giovan Battista Bellaso in 1553 (incorrectly attributed to Blaise de Vigenère centuries later). The Vigenère cipher improved significant weaknesses of the

Caesar cipher by using a sequence of Caesar ciphers, and the specific shift was determined based on a keyword. This polyalphabetic substitution made it much more difficult to break, and it became popularly known as "le chiffre indéchiffrable" (the indecipherable cipher) for three centuries. [6]



	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

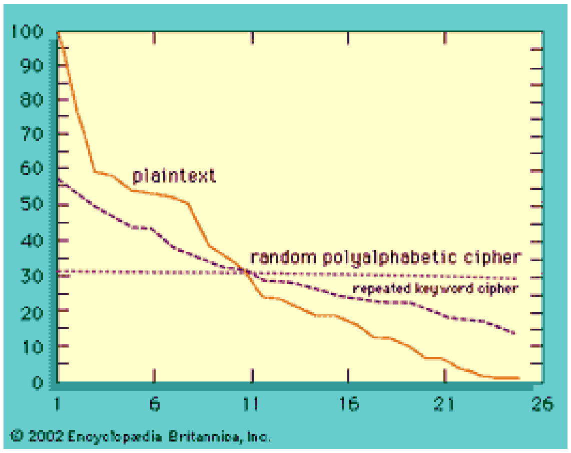
cipher	VVVRBACP
key	COVERCOVER...
plaintext	THANKYOU

In encrypting plaintext, the cipher letter is found at the intersection of the column headed by the plaintext letter and the row indexed by the key letter. To decrypt ciphertext, the plaintext letter is found at the head of the column determined by the intersection of the diagonal containing the cipher letter and the row containing the key letter.

© 2011 Encyclopædia Britannica, Inc.

Figure 4:Vigenère cipher

- The Vigenère cipher remained unbreakable until Friedrich Kasiski published a general technique for breaking it in 1863, a breakthrough in cryptanalysis. The breakthrough indicated how statistical analysis could be used to break even sophisticated classical ciphers, and cryptographers were forced to develop more complex systems.
- In the simplest systems of the Vigenère type, the key is a word or phrase that is repeated as many times as required to encipher a message. If the key is



© 2002 Encyclopædia Britannica, Inc.

Figure 5:letter frequency analysis of a Vigenère cipher. The text of this article was encrypted with a repeated-key Vigenère cipher—the key word is DECEPTIVE—and in a random polyalphabetic cipher. The figure shows how the relative frequency distribution of the original plaintext is disguised by the corresponding ciphertext, which more closely resembles a purely random sequence supplied as a baseline.

DECEPTIVE and the message is WE ARE DISCOVERED SAVE YOURSELF, then the resulting cipher will be [7]

```
Message : WE ARE DISCOVERED SAVE YOURSELF

Key     : DE CEP TIVEDECEPT IVED ECEPTIVE

Cipher  : ZI CVT WQNGRZGVTW AVZH CQYGLMGJ
```

- **Mechanical Era**
    - The turn of the 19th to the 20th century witnessed cryptography evolving with mechanical tools, of which the most infamous case was the Enigma machine. Created by German engineer Arthur Scherbius following World War I and used by the German forces in the 1920s, the Enigma utilized an electromechanical rotor system that encrypted the 26 letters of the alphabet.

    - Enigma's security relied on machine settings that were changed daily according to secret key lists, as well as settings that were changed for each message. It was so complicated that it was unbreakable at the time, and the Germans used it extensively during World War II to transmit military messages.

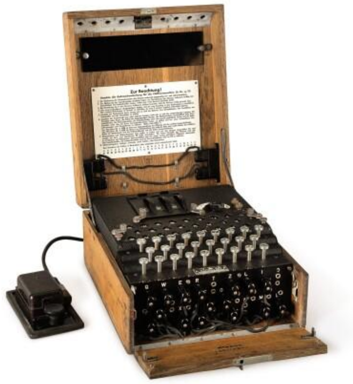


Figure 6:Enigma machine

    - The cracking of the Enigma code is one of the greatest achievements in cryptanalysis in history. Polish mathematicians Marian Rejewski first cracked early variants prior to the war, and British codebreakers at Bletchley Park (with Alan Turing among them) extended this effort. Their achievement has been credited with saving years off World War II and proved the critical strategic significance of cryptography and cryptanalysis. [8]

  - The other important cryptographic system of the era was the Lorenz cipher, used by Nazi Germany for high-level communications. Its breaking led to the development of Colossus, the world's first programmable electronic digital computer, by Tommy Flowers in 1943-1944. Colossus reduced decryption from weeks to hours, mirroring the growing nexus between computing and cryptography that would define the future of the discipline. [9]

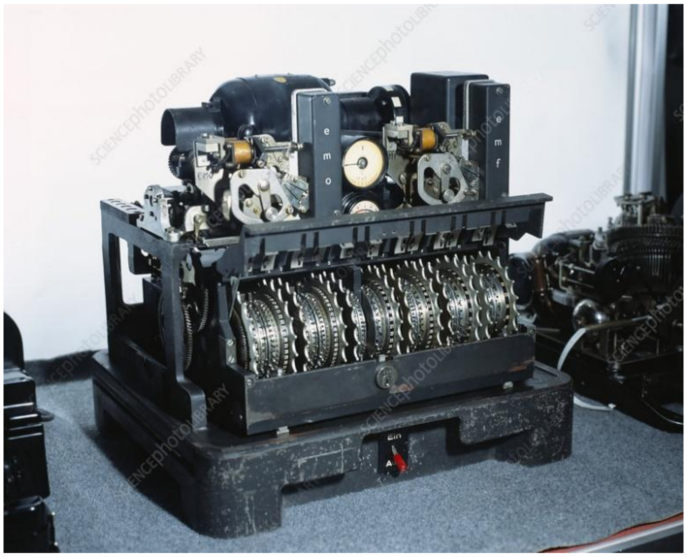


Figure 7:Lorenz cipher

- **Modern Computational Cryptography**
  - The development of computers during and after World War II transformed cryptography from an art to a mathematical science. Claude Shannon's seminal 1949 paper "Communication Theory of Secrecy Systems" gave the mathematical foundation of modern cryptography. Shannon's work has been described as "a turning point, marking the end of classical cryptography and the start of modern cryptography," transforming cryptography "from an art to a science.".

  - The paper introduced concepts that are still central to modern cryptography, like the confusion and diffusion principles on which secure cipher construction is founded. Shannon also theoretically proved that all theoretically unbreakable ciphers are no more demanding than the one-time pad, defining the theoretical limits of perfect secrecy.

- **Modern Symmetric Encryption**
  - The 1970s saw the creation of the Data Encryption Standard (DES) by IBM, which became a federal standard in 1977. DES was a significant step forward in encryption standardization, which encrypted 64-bit blocks of data using 56-bit keys and multiple rounds of substitution and permutation. [10]

  - Although revolutionary in its time, DES later became insecure with the increase in computing power. This led to the Advanced Encryption Standard (AES) contest by NIST in 1997. After rigorous analysis, the Rijndael algorithm developed by Belgian cryptographers Vincent Rijmen and Joan Daemen was selected as AES in 2001. [10] [11]

  - AES is used with 128-bit data blocks and key sizes of 128, 192, and 256 bits, which is far more secure than DES. It remains the standard for symmetric encryption to this day and is used in everything from secure comms to data protection and storage.

- **The Revolution of Public Key Cryptography**

  - Perhaps the most groundbreaking innovation in cryptography history was the creation of public-key cryptography in the 1970s. Before this innovation, all cryptographic schemes required the communicating parties to possess a shared secret key beforehand-great logistical issues for large-scale secure communications.

  - The innovation was idea-based in 1976 when Whitfield Diffie and Martin Hellman penned "New Directions in Cryptography," inventing public key cryptography. They supported a technique of key exchange (now referred to as the Diffie-Hellman key exchange) by which two parties can create a mutual secret key along an insecure link without sharing a mutual secret previously. [10]

  - The Diffie-Hellman protocol is based on the computational intractability of the discrete logarithm problem and allows parties to exchange public components which can be combined with private components to compute the same shared secret-without ever transmitting the secret itself.

  - Immediately following Diffie and Hellman's work, RSA algorithm was in 1977 invented by Ron Rivest, Adi Shamir, and Leonard Adleman with a complete public key cryptosystem. RSA's security is based on the realistic difficulty of factorizing the product of two enormous prime numbers into their factors. In RSA, users create a public key (made publicly available) and a private key (kept secret) such that messages encrypted using the public key can be decrypted using the corresponding private key.

  - Surprisingly, the same concepts had actually been conceived by the British spy organization GCHQ but were concealed. RSA basically was conceived by Clifford Cocks in 1973 and a similar key exchange method as Diffie-Hellman was conceived by Malcolm Williamson in 1974, but these only became public as recently as 1997.

- Public-key cryptography solved two fundamental problems: safe exchange of keys over insecure channels and digital signatures. Digital signature capability-providing authentication and non-repudiation its way into digital trust mechanisms as a necessary component, enabling secure e-commerce and electronic communication.

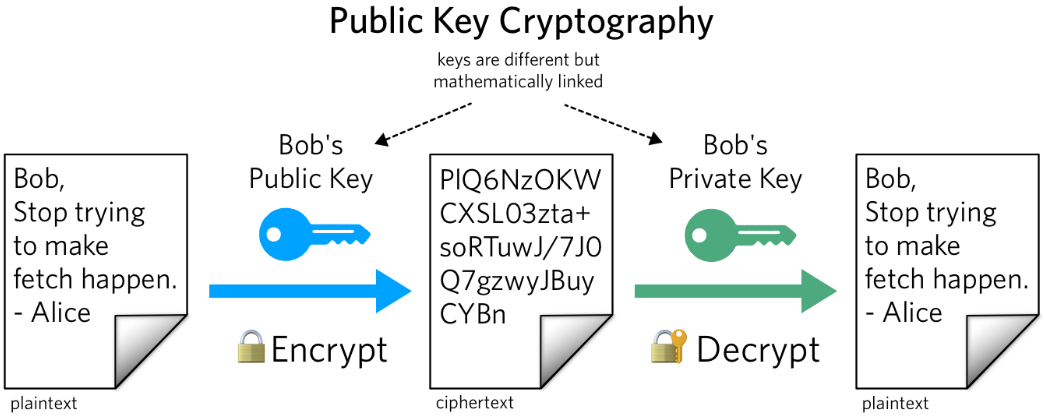


Figure 8:public key cryptography

- **Cryptography in the Internet Era**

  - The internet's exponential growth in the 1990s created new needs on cryptographic systems to supply security for communications in bulk. Netscape's Secure Sockets Layer (SSL) in 1994, and its successor Transport Layer Security (TLS), utilized symmetric and asymmetric cryptography in combination to enable secure communications on the internet. These protocols use public key cryptography for key exchange and authentication, before switching to symmetric encryption, which is faster, for the transmission of bulk data.

  - Pretty Good Privacy (PGP), written by Phil Zimmermann in 1991, brought strong cryptography to email. The subsequent legal battles when the U.S. government investigated Zimmermann for "exporting munitions" (as strong cryptography was then classified) highlighted cryptography's political dimensions and set the stage for the "crypto wars" of the 1990s.

  - The development of secure internet protocols enabled the progress of e-commerce, internet banking, and other sensitive internet transactions that require confidentiality, integrity, and authentication. The protocols continue to develop, with newer versions offering enhanced security and performance to fight new threats.

Era	Key Developments	Details
Ancient Cryptography	Non-standard hieroglyphics, early substitution ciphers	Egypt (1900 BC), Mesopotamia (encrypted recipes), Atbash cipher (600-500 BC)
Classical Cryptography	Caesar cipher, Augustus cipher, Vigenère cipher	Simple substitution, Vigenère (1553) was considered unbreakable until 1863
Mechanical Era	Enigma machine, Lorenz cipher	Enigma cracked by Bletchley Park (Turing), Colossus computer built for Lorenz
Modern Computational Cryptography	Formalization by Claude Shannon	1949 paper transformed cryptography into a science; introduced confusion and diffusion
Modern Symmetric Encryption	DES and AES	DES (1977) became obsolete; AES (2001) adopted, offering stronger encryption
Public Key Cryptography	Diffie-Hellman, RSA	Diffie-Hellman (1976), RSA (1977); solved secure key exchange and digital signatures
Cryptography in the Internet Era	SSL/TLS, PGP	SSL (1994) enabled secure web communication; PGP (1991) popularized secure email; led to "crypto wars" over cryptographic export controls

Figure 9: Summary of Evolution in Cryptography

3. Future Developments in Cryptography

As technology advances, cryptography is evolving to combat new threats and challenges. There are several emerging technologies and research fields that will likely shape the future of cryptography in the next couple of decades as a reaction to new opportunities and threats.

Post-Quantum Cryptography

Perhaps the largest and most significant challenge cryptography must contend with in the modern day is the very real threat posed by the ongoing development and the eventual realization of quantum computers. These cutting-edge supercomputers, which operate by using the advanced and groundbreaking principles of quantum mechanics to govern how they process information, possess the incredible capability of being able to break and decrypt easily a very vast majority of the existing cryptographic algorithms being utilized. Those founded on the hardness of mathematical problems, like RSA itself, founded on the hardness of integer factorization, and Diffie-Hellman, founded on the hardness of the discrete logarithm problem, will be more susceptible at the exact same time quantum computing has achieved practical maturity when it will be possible to use it everywhere.

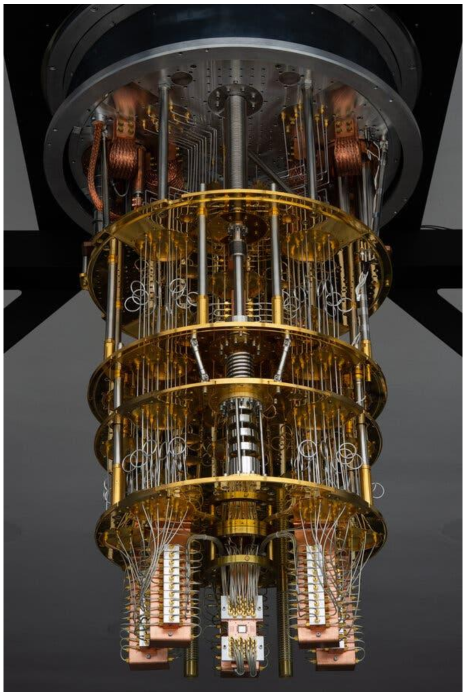


Figure 10: Quantum computer

Having become aware of the seriousness of this threat, the United States National Institute of Standards and Technology (NIST) initiated the Post-Quantum Cryptography Standardization project in 2016. The mission of this project is to research, select, and standardize new cryptographic primitives that would be secure against both classical computer attacks and quantum computer attacks.

In August 2024, NIST formally released its third set of finalized Post-Quantum Cryptography Standards: FIPS 203, FIPS 204, and FIPS 205. The standards are a breakthrough to enhance the security of digital infrastructure to prepare the world for the age of quantum computing.

Highlighting the historical importance and long-term implications of this project, NIST Deputy Secretary of Commerce Don Graves made a highly relevant remark when he stated, "The development of quantum computing is critical to restoring America's leadership as the world technology leader and building the future of our economic security." Not only does this remark highlight the inherent part that quantum computing must play in the field of technology but also its priceless contribution towards enabling the United States to remain abreast of the times and to secure its monetary security for decades to come.

Post-quantum cryptographic approaches include:

1. **Lattice-based cryptography**: Based on the computational hardness of solving certain problems in lattices, such as the shortest vector problem.
2. **Code-based cryptography**: Relying on the difficulty of decoding general linear codes.
3. **Hash-based cryptography**: Building security from the properties of cryptographic hash functions.
4. **Multivariate cryptography**: Using the difficulty of solving systems of multivariate polynomial equations.
5. **Isogeny-based cryptography**: Based on the complexity of finding isogenies between elliptic curves.

They are founded on fundamentally different mathematical principles from current public-key systems, with different security assumptions that are believed to be resistant to quantum attacks. The transition to these new algorithms is one of the largest cryptographic migrations ever and affects systems worldwide. [12] [13]

Quantum Key Distribution

While quantum computing does seriously threaten present-day cryptography, quantum mechanics does present new opportunities, one of the major ones being through Quantum Key Distribution (QKD). QKD allows two parties to compute a mutually agreed, secret, random key but only with knowledge known by these two parties. Subsequently, using regular algorithms, the parties can encrypt and decrypt information.

QKD makes use of a straightforward quantum mechanical truth: measuring a quantum system renders it transformed irreversibly. The fact makes eavesdropping identifiable since any intrication of the quantum states will make disturbances noticeable. QKD thereby offers the promise of provable secure communication regardless of interference from adversarial attackers.

Recently, QKD has undergone drastic advancement over the past several years. In 2024, Chinese and South African scientists made a discovery of a lifetime by conducting QKD across a record distance of 12,900 km. Employing lasers and a low Earth orbiting microsatellite, they sent more than one million quantum-secure bits between the two countries within a single satellite orbit. The breakthrough signals increasing practicality of QKD for secure communication around the world, an indicator of networks that are future-proofed against quantum attacks.

In 2023, researchers at the Indian Institute of Technology (IIT) Delhi have achieved a trusted-node-free quantum key distribution over 380 km of commercial telecom fiber with very low quantum bit error rates. These findings demonstrate QKD's growing practical applicability for securing communications even over large distances. Two main approaches to QKD have emerged:

1. **Prepare-and-measure protocols**: These exploit quantum indeterminacy, where measuring an unknown quantum state changes that state in a detectable way.
2. **Entanglement-based protocols**: These leverage quantum entanglement, where the quantum states of separate objects become linked such that measuring one affects the other, revealing any eavesdropping.

While systems of QKD are now being deployed in niche applications commercially, most notably for high-security environments, there remain difficulties to integrate QKD with existing network hardware and deploy it to global communications networks. [14] [15]

Homomorphic Encryption

Homomorphic encryption is one of the most fascinating subjects of active research in cryptography that can completely turn around how sensitive data gets processed, especially when it is in the cloud. The concept allows computations over encrypted data without violating confidentiality even after the processing process.

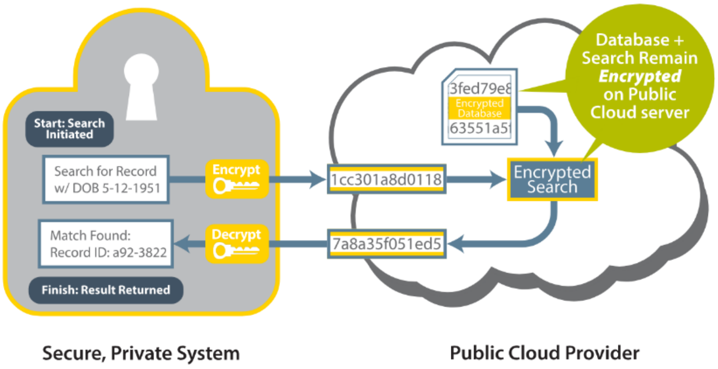


Figure 11;Homomorphic Encryption

For instance, an encrypted patient data could be stored on a cloud service by a hospital. The cloud can conduct calculations on encrypted data without ever decrypting and provide encrypted results, which become intelligible to the hospital once the output has been decrypted. Such a behavior utilizes the cloud for computation and enforces strong controls over sensitive information.

While partially homomorphic encryption schemes that allow for certain types of computation on encrypted information have been in existence for several years, progress was made in 2009 when Craig Gentry presented the first fully homomorphic encryption (FHE) scheme, which can facilitate arbitrary computation. A lot of work has been accomplished since then towards making FHE more practical, though there remain problems with efficiency and performance.

With improvements in homomorphic encryption technologies, they will continue to revolutionize industries like healthcare research, financial modeling, and privacy-respecting machine learning. These technologies can potentially enable companies to unleash the power of big data analytics without compromising privacy and security of sensitive data. [16] [17] [18]

Zero-Knowledge Proofs

Zero-knowledge proofs (ZKPs) allow a party to prove to another party that a statement is true without revealing anything except that the statement is in fact true. They are continually being made more efficient and resilient, and their value for privacy-preserving applications increases.

ZKPs have found particular use in blockchain and cryptocurrency, enabling private transactions that are confidential but can be verified. These technologies will find increasing use in the future for identity verification, secure voting mechanisms, and other applications where showing something without exposing sensitive information is desirable.

Recent advances in Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge (zk-SNARKs) and Zero-Knowledge Succinct Transparent Arguments of Knowledge (zk-STARKs) have made these proofs more efficient and practical for real-world applications, opening new possibilities for privacy-protecting verification systems. [16] [19]

Zero Knowledge Proofs
Prover
Secret Data & Proofs
Verifier

Figure 12: Zero Knowledge Proofs

Decentralized Identity and Cryptography

Based on blockchain technology and cryptographic building blocks, decentralized identity systems have been created with the aim of giving individuals full control over their own personal data. Decentralized identity systems use cryptographic tools to enable secure and controlled disclosure of identity attributes while ensuring security and privacy.

In contrast to traditional identity management, where personal data are stored in centralized databases and susceptible to being hacked, decentralized identity systems employ cryptographic proofs. It allows individuals to prove particular attributes—such as age, nationality, or qualifications—without showing extraneous personal details. Instead of exposing full identities, users are able to prove only the required information, reducing chances of data misuse.

Through the use of high-end cryptography like zero-knowledge proofs and digital signatures, decentralized identity systems present a more secure and private alternative to conventional identity verification. They eliminate the need to rely on third-party storage of data and allow individuals to possess their digital credentials directly.

With the leveraging of blockchain's transparency and immutability and the strength of cryptographic security measures, decentralized identity solutions represent an important milestone in the direction of empowering users, online trust enhancement, and constructing a more secure, user-centered digital identity framework.

Threshold Cryptography and Secure Multi-party Computation

Threshold cryptography supports cryptographic processes via cooperation from a number of parties. Threshold cryptography has also turned out to be a powerful resource in securing precious assets, confidential operations, and key management. Within the threshold system, one party is never completely in charge; instead, an appropriate number of players must cooperate for a valid digital signature or process. This eliminates the point of failure or breach, significantly boosting the security of the whole system.

By creating trust between participants, threshold cryptography enhances the security of a system against tampering and unauthorized access. Threshold cryptography is also widely used to secure sensitive infrastructures such as bitcoin wallets, certificate authorities, and other systems where it is required to protect private keys.

Extremely related to threshold cryptography is Secure Multi-Party Computation (MPC), or the technique of allowing several parties to jointly compute a function on their private inputs without revealing them to each other. For instance, several firms could share their customer data with an effort to calculate aggregate statistics without revealing customer information.

As MPC technologies progress, they are being used more and more in applications ranging from secure auctions to privacy-preserving machine learning and confidential data analysis. Such developments bring with them the possibility for new kinds of inter-organizational collaboration by making it possible to have joint computations without violating strict data privacy.

AI and Cryptography

Artificial intelligence (AI) can be anticipated to play a more important role in cryptography, both as a cryptanalytic tool as well as for the design and development of cryptographic systems. AI-based tools are being used more and more today to analyze cryptographic systems, detect vulnerabilities, and optimize system implementations to be more secure and efficient.

AI's interaction with cryptography is two-pronged. While AI may be used in the process of breaking or compromise of cryptographic security, cryptography itself has a core role to play in protecting AI-powered systems and sensitive information they depend on. As AI technologies become increasingly ubiquitous in mission-critical deployments, data confidentiality through strong cryptography is critical.

A good example is federated learning, which is a method of AI model training on multiple devices without requiring raw data movement. Federated learning enhances both privacy and security during training by keeping data local and utilizing cryptographic techniques to protect the data.

One such area of promise is the meeting point between cryptography and artificial intelligence. It is possible to utilize this point of intersection to construct more secure cryptographic systems along with enhancing the privacy of AI systems, both contextually and cryptographically. As both the areas continue developing alongside each other, they offer new possibilities in enhancing secure, privacy-preservation technologies. [16] [20]

Quantum-Safe Hybrid Systems

As more and more quantum resistant algorithms standardize and get released into the market we will see a hybrid of traditional cryptography and post quantum cryptography implemented in many systems. The hybrid cryptographic suite paradigm allows for some defense in depth; if one type of encryption gets compromised the other could be rendered resilient.

The case for hybrid systems is likely to be particularly relevant in the transitional period, when quantum computers become more powerful, but nuclear hybrid post-quantum cryptography is not yet considered to be field testable; hybrid implementation of both class of algorithms at the same time gives organizations the opportunity to realize backward compatibility and guarantees their readiness for a quantum world.

In fact many of the most popular internet browsers and server software vendors are already working on implementing hybrid cryptographic suites that would make it easier than ever to transition to quantum safe algorithms once widespread use of post - quantum algorithms has been achieved and it is possible to move away from traditional cryptographic algorithms. [21] [22]

4. Conclusion

Cryptography has evolved, from primitive substitution codes carved into the walls of Egyptian tombs to super-sophisticated mathematical systems now securing our most intimate digital communications. This progress is not only due to an ongoing requirement for communication privacy, but also due to an ongoing intellectual struggle between those who create secure systems and those who attempt to break them.

From Caesar cipher to the dawn of post-quantum cryptography, history of encryption has seen technological advancement as well as greater mathematical insight. From being an art carried out by diplomats and soldiers, the encryption has now evolved into a serious scientific discipline. Claude Shannon's contribution was instrumental in changing cryptography as a science grounded on formal theories and provable security assurances.

Through the years, cryptography has had to adapt to new technology and new threats. When the first classical ciphers were brought down by methods such as frequency analysis, it triggered innovation in constructing ciphers. Same thing with the Enigma machine and the gargantuan amount of computation that eventually broke it. Nowadays, quantum computing looms as the next great plague, challenging scientists to create new types of cryptography resilient to previously unimaginable computational might.

And yet another crucial transition has been toward open cooperation. What had previously been the sole province of secret military and intelligence organizations, cryptography is today defined by worldwide cooperation and open competition. NIST-style institutions drive standards creation by open mechanisms, making international calls to solicit experts to discover vulnerabilities early and make designs tough through open comment.

In the years ahead, cryptography will face some of its largest challenges yet. Quantum computers are pledged to be able to compromise the public-key schemes that presently defend most communications across the internet. But researchers are fighting back with new ideas—post-quantum cryptographic techniques and even quantum key agreement plans—that might shield information in a post-quantum age.

In addition to getting ready for quantum attacks, cryptography is also growing to address new requirements. Homomorphic encryption would allow sensitive information to be computed without damaging it. Zero-knowledge proofs are making possible methods of proving data without revealing confidential information. Decentralized identity technology is being developed to enable people to better control their personal information using cryptographic techniques. These technologies are most likely going to change the way we consider privacy and data protection over the next several decades.

More than ever, cryptography is the invisible foundation of contemporary society. It safeguards everything from internet transactions to secret chats, from software update authentication to digital identity protection. As our dependence on digital infrastructure increases, so does the need for robust, reliable cryptography.

In an age in which surveillance and information gathering are more ubiquitous than ever before, cryptography remains a vital protector of privacy and freedom. Its future is as much a matter of technological progress as one of deep philosophical necessity concerning issues of individual liberty, security, and trust in the computer era. As we go forward, continued research in cryptographic techniques will be crucial to the preservation of a free and secure society's most fundamental tenets.

5. References

[1] "Cryptography," 03 April 2025. [Online]. Available: https://en.wikipedia.org/wiki/Cryptography.

[2] "History of Cryptography," 13 April 2025. [Online]. Available: https://en.wikipedia.org/wiki/History_of_cryptography.

[3] M. K. G. Adomey, "Introduction to Cryptography," [Online]. Available: //www.itu.int/en/ITU-D/Cybersecurity/Documents/01-Introduction%20to%20Cryptography.pdf .

[4] ""Caesar cipher | History, Method, Examples, Security, & Facts,"," 11 April 2025. [Online]. Available: https://www.britannica.com/topic/Caesar-cipher.

[5] "An Abridged History of Cryptography Caesar Cipher Vigenère Cipher University of Washington," [Online]. Available: https://courses.cs.washington.edu/courses/cse490h1/19wi/exhibit/artifacts/crypto.pdf.

[6] M. 7. 2. [. A. CodedInsights, ""The Vigenère Cipher - CodedInsights,"," 7 March 2024. [Online]. Available: https://codedinsights.com/classical-cryptography/vigenere-cipher/.

[7] G. J. Simmons, "Vigenère cipher," 11 April 2025. [Online]. Available: https://www.britannica.com/topic/Vigenere-cipher.

[8] "Enigma machine," 23 April 2025. [Online]. Available: https://en.wikipedia.org/wiki/Enigma_machine.

[9] "The History of the Lorenz Cipher and the Colossus Machine," [Online]. Available: https://cs.stanford.edu/people/eroberts/courses/soco/projects/2008-09/colossus/history.html.

[10] "The Evolution of AES," 1 November 2023. [Online]. Available: https://www.ghostvolt.com/blog/the-history-of-aes-encryption.html.

"A NIST-Based Summary of Cryptographic Algorithms," 27 December 2019. [Online]. Available: https://www.cryptomathic.com/blog/summary-of-cryptographic-algorithms-according-to-nist.

[12] "NIST Post-Quantum Crytograohy Standardization," 19 March 2025. [Online]. Available: https://en.wikipedia.org/wiki/NIST_Post-Quantum_Cryptography_Standardization.

[13] "NIST Releases First 3 Finalized Post-Quantum Encryption Standards," 13 August 2024. [Online]. Available: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards.

[14] "Artificial intelligence and quantum cryptography," 2024. [Online]. Available: https://jast-journal.springeropen.com/articles/10.1186/s40543-024-00416-6.

[15] "Quantum key distribution," 29 April 2025. [Online]. Available: https://en.wikipedia.org/wiki/Quantum_key_distribution.

[16] jamesbachini, "The Future Of Cryptography," [Online]. Available: https://jamesbachini.com/future-of-cryptography/.

[17] "Homomorphic Encryption," 1 April 2025. [Online]. Available: https://en.wikipedia.org/wiki/Homomorphic_encryption.

[18] "Homomorphic Encryption," 18 Octomber 2023. [Online]. Available: https://www.geeksforgeeks.org/homomorphic-encryption/.

[19] "Zero-knowledge proof," 30 April 2025. [Online]. Available: https://en.wikipedia.org/wiki/Zero-knowledge_proof.

[20] S. Ambassadors, "AI Cryptography: Enhancing Security and Privacy in the Digital Age," 7 Octomber 2023. [Online]. Available: https://medium.com/@singularitynetambassadors/ai-cryptography-enhancing-security-and-privacy-in-the-digital-age-db5c1bbf5fdb.

[21] S. Antipolis, "ETSI launches new standard for Quantum-Safe Hybrid Key Exchanges to secure future post-quantum encryption," 25 March 2025. [Online]. Available: https://www.etsi.org/newsroom/press-releases/2513-etsi-launches-new-standard-for-quantum-safe-hybrid-key-exchanges-to-secure-future-post-quantum-encryption#:~:text=The%20specification%20%E2%80%9CEfficient%20Quantum%2DSafe,sensitive%20data%20to%20decrypt%2.

[22] "Will Hybrid Cryptography Protect Us from the Quantum Threat?," 06 June 2019. [Online]. Available: https://cloudsecurityalliance.org/blog/2019/06/17/hybrid-cryptography-quantum-threat.