Evolution of Cryptography

Cryptography, the use of codes and ciphers to protect secrets, began thousands of years ago. Until recent decades, it has been the story of what might be called classical cryptography — that is, of methods of encryption that use pen and paper, or perhaps simple mechanical aids. In the early 20th century, the invention of complex mechanical and electromechanical machines, such as the Enigma rotor machine, provided more sophisticated and efficient means of encryption; and the subsequent introduction of electronics and computing has allowed elaborate schemes of still greater complexity, most of which are entirely unsuited to pen and paper.

by Pratham Borghare(241059005)

Early Cryptography

1

Ancient Egypt

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. These are not thought to be serious attempts at secret communications, however, but rather to have been attempts at mystery, intrigue, or even amusement for literate onlookers.

2

Mesopotamia

Some clay tablets from Mesopotamia somewhat later are clearly meant to protect information—one dated near 1500 BC was found to encrypt a craftsman's recipe for pottery glaze, presumably commercially valuable.

3

Hebrew

Furthermore, Hebrew scholars made use of simple monoalphabetic substitution ciphers (such as the Atbash cipher) beginning perhaps around 600 to 500 BC.

4

India

In India around 400 BC to 200 AD, Mlecchita vikalpa or "the art of understanding writing in cypher, and the writing of words in a peculiar way" was documented in the Kama Sutra for the purpose of communication between lovers. This was also likely a simple substitution cipher.

Ancient Greece and Rome

1

Scytale

The ancient Greeks are said to have known of ciphers. The scytale transposition cipher was used by the Spartan military, but it is not definitively known whether the scytale was for encryption, authentication, or avoiding bad omens in speech.

2

Polybius Square

Another Greek method was developed by Polybius (now called the "Polybius Square").

3

Caesar Cipher

The Romans knew something of cryptography (e.g., the Caesar cipher and its variations).

Medieval Cryptography

Arab Contributions

David Kahn notes in _The Codebreakers_ that modern cryptology originated among the Arabs, the first people to systematically document cryptanalytic methods. Al-Khalil (717–786) wrote the _Book of Cryptographic Messages_, which contains the first use of permutations and combinations to list all possible Arabic words with and without vowels.

Frequency Analysis

The invention of the frequency analysis technique for breaking monoalphabetic substitution ciphers, by Al-Kindi, an Arab mathematician, sometime around AD 800, proved to be the single most significant cryptanalytic advance until World War II.

Medieval England

In early medieval England between the years 800–1100, substitution ciphers were frequently used by scribes as a playful and clever way to encipher notes, solutions to riddles, and colophons.

Renaissance Cryptography

1

Alberti's Polyalphabetic Cipher

Essentially all ciphers remained vulnerable to the cryptanalytic technique of frequency analysis until the development of the polyalphabetic cipher, and many remained so thereafter. The polyalphabetic cipher was most clearly explained by Leon Battista Alberti around AD 1467, for which he was called the "father of Western cryptology".

2

Trithemius' Tabula Recta

Johannes Trithemius, in his work Poligraphia, invented the tabula recta, a critical component of the Vigenère cipher. Trithemius also wrote the “Steganographia”.

3

Bellaso's Vigenère Cipher

Giovan Battista Bellaso in 1553 first described the cipher that would become known in the 19th century as the Vigenère cipher, misattributed to Blaise de Vigenère.

Cryptography in the 1800s

Babbage's Cryptanalysis

Examples of the latter include Charles Babbage's Crimean War era work on mathematical cryptanalysis of polyalphabetic ciphers, redeveloped and published somewhat later by the Prussian Friedrich Kasiski.

Kerckhoffs' Cryptographic Writings

Understanding of cryptography at this time typically consisted of hard-won rules of thumb; see, for example, Auguste Kerckhoffs' cryptographic writings in the latter 19th century.

Edgar Allan Poe's Cryptography

Edgar Allan Poe used systematic methods to solve ciphers in the 1840s. In particular he placed a notice of his abilities in the Philadelphia paper _Alexander's Weekly (Express) Messenger_, inviting submissions of ciphers, most of which he proceeded to solve.

World War I Cryptography

1

Room 40

In World War I the Admiralty's Room 40 broke German naval codes and played an important role in several naval engagements during the war, notably in detecting major German sorties into the North Sea that led to the battles of Dogger Bank and Jutland as the British fleet was sent out to intercept them.

2

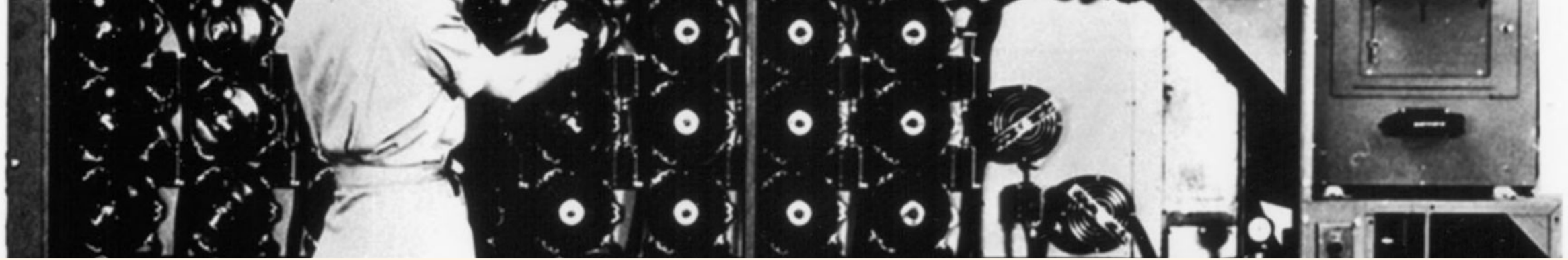
Zimmermann Telegram

However, its most important contribution was probably in decrypting the Zimmermann Telegram, a cable from the German Foreign Office sent via Washington to its ambassador Heinrich von Eckardt in Mexico which played a major part in bringing the United States into the war.

3

Vernam's Teleprinter Cipher

In 1917, Gilbert Vernam proposed a teleprinter cipher in which a previously prepared key, kept on paper tape, is combined character by character with the plaintext message to produce the ciphertext.



World War II Cryptography

Germany

The Germans made heavy use, in several variants, of an electromechanical rotor machine known as Enigma.

Poland

Mathematician Marian Rejewski, at Poland's Cipher Bureau, in December 1932 deduced the detailed structure of the German Army Enigma, using mathematics and limited documentation supplied by Captain Gustave Bertrand of French military intelligence acquired from a German clerk.

Britain

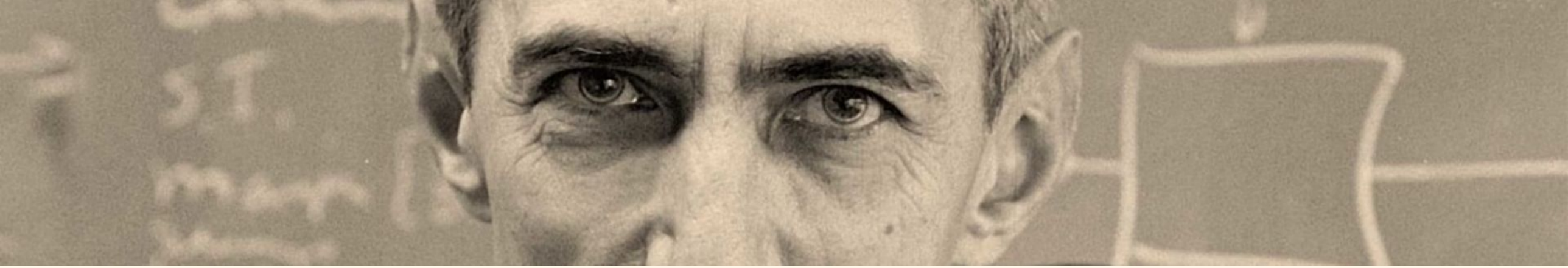
Soon after the invasion of Poland by Germany on 1 September 1939, key Cipher Bureau personnel were evacuated southeastward; on 17 September, as the Soviet Union attacked Poland from the East, they crossed into Romania.

Japan

A US Army group, the SIS, managed to break the highest security Japanese diplomatic cipher system (an electromechanical stepping switch machine called Purple by the Americans) in 1940, before the attack on Pearl Harbour.

Modern Cryptography

DES	Data Encryption Standard
AES	Advanced Encryption Standard
SSL	Secure Socket Layer



Claude Shannon's Contributions

1

Mathematical Theory of Cryptography

Claude E. Shannon is considered by many to be the father of mathematical cryptography. Shannon worked for several years at Bell Labs, and during his time there, he produced an article entitled "A mathematical theory of cryptography".

2

Unbreakable Cipher

Shannon identified the two main goals of cryptography: secrecy and authenticity. His focus was on exploring secrecy and thirty-five years later, G.J. Simmons would address the issue of authenticity.

3

Transition from Art to Science

Shannon wrote a further article entitled "A mathematical theory of communication" which highlights one of the most significant aspects of his work: cryptography's transition from art to science.