The Innovation of Cryptology: An Enigma of History

http://www.youtube.com/watch?v=nwjEOipRWbU

Pre-listening:

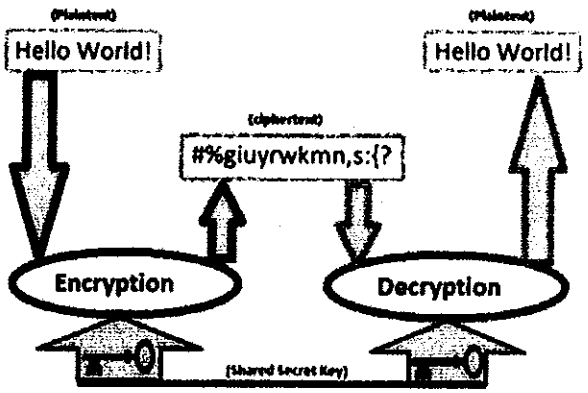
1. **What is cryptology and where is it used?**
2. **Do you know what an enigma or the Enigma is?**
3. **What do these expressions mean: to crack a message, to encrypt a message, to intercept a message**

Listening. Answer Qs.

1) Which uses of cryptology does the speaker mention?
.....
2) What is the difference between Cryptoanalysis and Cryptography?
.....
3) What is the difference between Code and Cipher and which of them is more widely used?
.....
4) Who was the first to use Cryptology? .....
5) Why was Cryptology important during the American Revolution?
.....
6) What were the consequences of the Zimmerman telegram?
.....
7) When was the Enigma code cracked and by whom? .....
8) Why was cracking the Enigma code important? .....

Cryptography

From Wikipedia, the free encyclopedia



Read the text and answer questions.

1. Who are adversaries and what should overcome their influence?
2. What was the widespread use of cryptology enabled by?
3. What does it mean when the scheme is computationally secure?

Cryptography (or *cryptology*; from Greek κρυπτός, "hidden, secret"; and γράφειν, *graphein*, "writing", or -λογία, *-logia*, "study", respectively) is the practice and study of techniques for secure communication in the presence of third parties (called adversaries). More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, and authentication. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

Cryptography prior to the modern age was effectively synonymous with *encryption*, the conversion of information from a readable state to apparent nonsense. The originator of an encrypted message shared the decoding technique needed to recover the original information only with intended recipients, thereby precluding unwanted persons to do the same. Since World War I and the advent of the computer, the methods used to carry out cryptology have become increasingly complex and its application more widespread.

Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary. It is theoretically possible to break such a system but it is infeasible to do so by any known practical means. These schemes are therefore termed computationally secure; theoretical advances (e.g., improvements in integer factorization algorithms) and faster computing technology require these solutions to be continually adapted. There exist information-theoretically secure schemes that provably cannot be broken even with unlimited computing power—an example is the one-time pad—but these schemes are more difficult to implement than the best theoretically breakable but computationally secure mechanisms.

Terminology

Explain the difference between:

a) Plaintext and Ciphertext
b) Encryption and Decryption
c) Code and Cipher
d) Cryptography and Cryptology
e) Algorithm and key

Until modern times cryptography referred almost exclusively to *encryption*, which is the process of converting ordinary information (called plaintext) into unintelligible gibberish (called ciphertext). Decryption is the reverse, in other words, moving from the unintelligible ciphertext back to plaintext. A *cipher* (or *cypher*) is a pair of algorithms that create the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and in each instance by a "key". This is a secret parameter (ideally known only to the communicants) for a specific message exchange context. A "cryptosystem" is the ordered list of elements of finite possible plaintexts, finite possible cyphertexts, finite possible keys, and the encryption and decryption algorithms which correspond to each key. Keys are important, as ciphers without variable keys can be trivially broken with only the knowledge of the cipher used and are therefore useless (or even counter-productive) for most purposes. Historically, ciphers were often used directly for encryption or decryption without additional procedures such as authentication or integrity checks.

In colloquial use, the term "code" is often used to mean any method of encryption or concealment of meaning. However, in cryptography, *code* has a more specific meaning. It means the replacement of a unit of plaintext (i.e., a meaningful word or phrase) with a code word (for example, `wallaby` replaces `attack at dawn`). Codes are no longer used in serious cryptography—except incidentally for such things as unit designations (e.g., Bronco Flight or Operation Overlord)—since properly chosen ciphers are both more practical and more secure than even the best codes and also are better adapted to computers.

Cryptanalysis is the term used for the study of methods for obtaining the meaning of encrypted information without access to the key normally required to do so; i.e., it is the study of how to crack encryption algorithms or their implementations.

Some use the terms *cryptography* and *cryptology* interchangeably in English, while others (including US military practice generally) use *cryptography* to refer specifically to the use and practice of cryptographic techniques and *cryptology* to refer to the combined study of cryptography and cryptanalysis. English is more flexible than several other languages in which *cryptology* (done by cryptologists) is always used in the second sense above. In the English Wikipedia the general term used for the entire field is *cryptography* (done by cryptographers).