MEETING 11

CRYPTOGRAPHY

What is Cryptography

The term cryptography is derived from Greek, kryptos means “hidden” or “secret” and graphy means “writing”. So, cryptography is the practice and study of creating a secret information.
Cryptography works by Cryptography is a part of mathematics and computer science.

Continued

Cryptography is used in applications present in technologically advanced societies; examples include the security of ATM cards, computer passwords, and electronic commerce, which all depend on cryptography. In short we can say that cryptography is needed to secure a secret document. A person who is master in cryptography is called cryptographer.

How Cryptography Works

For example someone has a secret document to secure. Any document can be secured using cryptography. For example we have to secure the word “Read” using cryptography. The word “Read” in cryptography is called Plain text. Using a set of rule called algorithm, the plain text is changed into cipher text. This process is called encryption. The result of this encryption process is the word “Uhdg”. This is the cipher text.

History of Cryptography

Cryptography is already used since ancient era. Julius Caesar used cryptography to secure his message from his enemy. He replaced a character with its next three character. For example a character ‘A’ in alphabet will be replaced by character ‘D’. And so on. See the list below of Julius Caesar algorithm.

Examples :

- **Plain text : 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**
- **Cipher Text : 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**

Continued History

In the era of World War II, German Nazi was also used cryptography to secure its message. Nazi used a machine called Enigma to encrypt and decrypt the messages. In this way Nazi thought its message would be difficult to break by US and its allies. Below is a picture of Enigma used by Nazi. Unfortunately the algorithm of Enigma can be broken by US army.

Continued History

In computer technology, cryptography is still used to secure a computer data or document. For example in ATM machine,computer passwords, and also in electronic commerce. Using computer technology someone can use many sophisticated algorithm for example RSA,DES, and PGP.

Computer Terms

- Plain text = a text that can be read by anybody. This text is not secured yet.
- Cipher text = a secret text resulting from encryption process.
- Algorithm = a set of rule to encrypt a document.
- Enigma = a machine like typewriter that is used by Nazi during World War II to secure a document before transmitted.
- Cryptographer = a person who is master in cryptography.

Exercises Meeting-11

1. What is cryptography ….
2. What is the different between cryptography and steganography ….
3. How the cryptography works ….
4. Give the example of cryptography …
5. Give the example using cryptography in computer technology …

Exercises Meeting-11

1. The practice and study of creating a secret information.
   a. Stenography
   b. Crytography
   c. Steganomy
   d. Stagenoghrapy
   e. All answer are false
2. A cryptography is used in applications present in technologically advanced societies, the examples…
   a. Security of ATM cards
   b. Computer passwords
   c. Electronic commerce A message
   d. A,B and C true
   e. Hidden Mesagge
3. A machine called Enigma to encrypt and decrypt the messages in worl war II used by…
   a. German
   b. America
   c. France
   d. Italy
   e. Russia
4. The example of cryptography …
   a. Greek
   b. Enigma
   c. Enogmist
   d. Login
   e. A,B and C true
5. The a secret text resulting from encryption process is ….
   a. Hidden Writing
   b. Chiper text
   c. Hidden text
   d. A and B true
   e. No Answer

References

- http://en.wikipedia.org/wiki/Cryptography
- http://en.wikipedia.org/wiki/Cryptography_Classification
- http://en.wikipedia.org/wiki/Encyclopedia_of_Cryptography_and_Security
- http://en.wikipedia.org/wiki/Japanese_cryptology_from_the_1500s_to_Meiji
- http://en.wikipedia.org/wiki/List_of_important_publications_in_computer_science#Cryptography
- http://www.merriam-webster.com/dictionary/cryptology/
- http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf
- http://www.cesg.gov.uk/site/publications/media/notense.pdf
- http://citeseer.ist.psu.edu/cache/papers/cs/22094/http:zSzzSzeprint.iacr.orgzSz2001zSz056.pdf/junod01complexity.pdf
- http://www.rsasecurity.com/rsalabs/node.asp?id=2152
- http://www.ieee-security.org/Cipher/Newsbriefs/1996/960214.zimmerman.html
- http://www.schneier.com/crypto-gram-0006.html#DES
- http://scholar.google.com/url?sa=U&q=http://www.springerlink.com/index/K54H077NP8714058.pdf
- http://www.cacr.math.uwaterloo.ca/hac/
- http://www.cryptool.org/download/CrypToolPresentation-en-1_4_20.pdf
- http://www.rsasecurity.com/rsalabs/node.asp?id=2152
- http://www.pawlan.com/Monica/crypto/
- http://www.nsa.gov/kids/

