Cryptography Basics

Cryptography

- History
- Basic terminologies
- Symmetric key encryption
- Asymmetric key encryption
- Public Key Infrastructure

History

- 50 B.C. Julius Caesar uses cryptographic technique
- 400 A.D. Kama Sutra in India mentions cryptographic techniques
- 1250 British monk Roger Bacon describes simple ciphers
- 1466 Leon Alberti develops a cipher disk
- 1861 Union forces use a cipher during Civil War

History

- 1914 World War I – British, French, and German forces use encryption technology
- 1917 William Friedman, Father of U.S. encryption efforts starts a school for teaching cryptanalysis in Illinois
- 1917 AT&T employee Gilbert Vernam invents polyalphabetic cipher
- 1919 Germans develop the Engima machine for encryption

History

- 1937 Japanese design the Purple machine for encryption
- 1942 Navajo windtalkers help with secure communication during World War II
- 1948 Claude Shannon develops statistical methods for encryption/decryption
- 1976 IBM develops DES
- 1976 Diffie – Hellman develop public key / private key cryptography
- 1977 Rivest – Shamir – Adleman develop the RSA algorithm for public key / private key

Basic Terminologies

- Cryptography deals with creating documents that can be shared secretly over public communication channels
- Cryptographic documents are decrypted with the key associated with encryption, with the knowledge of the encryptor
- The word cryptography comes from the Greek words: Krypto (secret) and graphein (write)
- Cryptanalysis deals with finding the encryption key without the knowledge of the encryptor
- Cryptology deals with cryptography and cryptanalysis
- Cryptosystems are computer systems used to encrypt data for secure transmission and storage

Basic Terminologies

- Keys are rules used in algorithms to convert a document into a secret document
- Keys are of two types:
  - Symmetric
  - Asymmetric
- A key is symmetric if the same key is used both for encryption and decryption
- A key is asymmetric if different keys are used for encryption and decryption

Basic Terminologies

- Examples:
  - Symmetric key methods
    - DES 56-bit
    - Triple DES 128-bit
    - AES 128-bit and higher
    - Blowfish 128-bit and higher
  - Asymmetric key methods
    - RSA (Rivest-Shamir-Adleman of MIT)
    - PGP (Phil Zimmerman of MIT)

Basic Terminologies

- Plaintext is text that is in readable form
- Ciphertext results from plaintext by applying the encryption key
- Notations:
  - M message, C ciphertext, E encryption, D decryption, k key
  - E(M) = C
  - E(M, k) = C
- Fact: D(C) = M, D(C, k) = M

Basic Terminologies

- Hash functions generate a digest of the message
- Substitution cipher involves replacing an alphabet with another character of the same alphabet set
- Mono-alphabetic system uses a single alphabetic set for substitutions
- Poly-alphabetic system uses multiple alphabetic sets for substitutions
- Caesar cipher is a mono-alphabetic system in which each character is replaced by the third character in succession. Julius Caesar used this method of encryption.