Basics of Cryptography

[version 1]
Date: April 7, 2010

Author: Amber Jain (ithinkminus [at] gmail)
For project: Cryptic (http://cryptic.sourceforge.net/)

The latest version of this document is linked from:
http://cryptic.sourceforge.net/documentation.html

TERMINOLOGIES:

- A message is **plaintext** (sometimes called cleartext). The process of disguising a message in such a way as to hide its substance is **encryption**. An encrypted message is **ciphertext**. The process of turning ciphertext back into plaintext is **decryption**.

- A **cryptographic algorithm**, also called a **cipher**, is the mathematical function used for encryption and decryption.

- The art and science of keeping messages secure is **cryptography**, and it is practiced by **cryptographers**. **Cryptanalysts** are practitioners of **cryptanalysis**, the art and science of breaking ciphertext; that is, seeing through the disguise. The branch of mathematics encompassing both cryptography and cryptanalysis is **cryptology** and its practitioners are **cryptologists**.

- There are two general types of key-based algorithms: **symmetric** and **public-key:**

  Symmetric algorithms, sometimes called conventional algorithms, are algorithms where the encryption key can be calculated from the decryption key and vice versa. In most symmetric algorithms, the encryption key and the decryption key are the same. These algorithms, also called secret-key algorithms, single-key algorithms, or one-key algorithms, require that the sender and receiver agree on a key before they can communicate securely. The security of a symmetric algorithm rests in the key; divulging the key means that anyone could encrypt and decrypt messages. As long as the communication needs to remain secret, the key must remain secret.

  Public-key algorithms (also called asymmetric algorithms) are designed so that the key used for encryption is different from the key used for decryption. Furthermore, the decryption key cannot (at least in any reasonable amount of time) be calculated from the encryption key. The algorithms are called public-key because the encryption key can be made public: A complete stranger can use the encryption key to encrypt a message, but only a specific person with the corresponding decryption key can decrypt the message. In these systems, the encryption key is often called the public key, and the decryption key is often called the private key.

  Public key or asymmetric cryptographic algorithms usually take a lot of computation time and memory as compared to symmetric ciphers. In most cases, symmetric ciphers are recommended for data encryption (and decryption) unless the user is willing to spend very large amount of computational effort to encryption/decryption using public key cipher. Public key ciphers are recommended to be used only in situations such as authentication or to confidentially distribute symmetric keys.

- A **cryptographic hash function** is a *deterministic procedure* that takes an arbitrary block of *data* and returns a fixed-size *bit* string, the (**cryptographic**) **hash value**, such that an accidental or intentional change to the data will change the hash value. The data to be encoded is often called the "message", and the hash value is sometimes called the **message digest** or simply **digest**.
  Cryptographic hash functions have many information security applications, notably in digital signatures, message authentication codes (MACs), and other forms of authentication.

They can also be used as ordinary hash functions, to index data in hash tables, for fingerprinting, to detect duplicate data or uniquely identify files, and as checksums to detect accidental data corruption.

- Password Safe is a program that inputs:
  * a master passwords
  * List of user's login Ids and passwords for various types of accounts
  The program locks all the loginIDs/passwords using master password so that user needs to remember only one password for login information for all other accounts.

- **Important**: The data to be encrypted/decrypted can be any kind of data (text, audio, video, image etc.)

- At very basic level, cryptography does following jobs:
  0. **Confidentiality**: No one except intended receiver should be ablle to read contents of message. This is encryption/decryption.

  1. **Integrity**: It should be possible for the receiver of a message to verify that it has not been modified in transit; an intruder should not be able to substitute a false message for a legitimate one. This is hashing.

- *Question*: Do average people really need this kind of security?
  OR
  Do I really need to secure my data?
  Answer: Yes. They may be planning a political campaign, discussing taxes, or having an illicit affair. They may be designing a new product, discussing a marketing strategy, or planning a hostile business takeover. Or they may be living in a country that does not respect the rights of privacy of its citizens. They may be doing something that they feel shouldn't be illegal, but is. For whatever reason, the data and communications are personal, private, and no one else's business.

NOTE: You can read Applied Cryptography (by Bruce Scheiner) [1] in Bibliography (at the end of this document) for more details about cryptography.

BIBLIOGRAPHY:

1. Applied Cryptography (Bruce Scheiner) http://www.schneier.com/book-applied.html
2. Wikipedia