Internet technology
MD. Rasel Hossain
ID-163432521
Assignment

Cryptography and Information Security

Introduction: The science concerned with communications in secure and usally secret form. It encompasses both cryptography and cryptanalysis. The former involves the study and application of the principles and techniques by which information is rendered unintelligible to all but the intended receiver while the latter is the science and art of solving cryptography to recover such information

information protection covers not only secrecy but also.

- Authentication.
- Integrity
- Verifiability
- Non-repudiation and other security goals

To incorporate information protection into a system the designer need to know:

* a detailed specification of the environment
* a list of threats.
* The level of protection required or amount of power that is expected from an adversary.

* The projected life span of the system.

cryptography provides our design with tools to achieve the security goals expected.

The collection of basic tools includes.

* encryption algorithm
* authentication codes
* one-way functions
* secret-sharing schemes.
* signature schems etc.

* More complex tools and services:
  * authentication protocols.
  * key establishment protocols
  * variety of application protocols.
    - electronic payment systems
    - electronic election.

Terminology

Basic Security requirments:

- confidentially/secrecy
- Authenticaty
- Integrity.
- Non-repudiation
- message/plaintext.
- Encryption
- cryptogram/ciphertext
- Decryption
- Encryption/Decryption algorithm
- ciphers/cryptoalgorithm/cryptosystems
- private-Key or Symmetric CryptoSystem
- public-Key or asymmetric cryptosystem.
- Hashing
- one-way functions

- Electronic signature
- Secret sharing.

Cryptanalysis has its own terminology as well.

- unconditionally secure.
- conditionally secure
- attack
- exhaustive search attack.

Encryption algorithm can be analysed using the following typical attacks.

* Ciphertext - only attack
* Known - plaintext attack
* chosen - plaintext attack
* chosen - ciphertext attack.

Authentication algorithm can be evaluated using their resistance against the following attack.

* Impersonation attack
* Substitution attack
* Spoofing attack

All hashing algorithm are susceptible to

* collision
* birthday-attack
* pseudo-collision.