Cryptography and Information Security

Md Mokammel Haque, PhD

CUET

July 18, 2016

Table of Contents

Table of Contents

Introduction

New Encyclopedia Britannica defined *Cryptology* as: "The science concerned with communications in secure and usually 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 cryptosystems to recover such information."

Introduction

Information protection covers not only secrecy (a traditional protection against eavesdropping) but also

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

Introduction

Information protection covers not only secrecy (a traditional protection against eavesdropping) but also

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

Introduction

Information protection covers not only secrecy (a traditional protection against eavesdropping) but also

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

Introduction

Information protection covers not only secrecy (a traditional protection against eavesdropping) but also

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

Introduction

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

- a detailed specification of the environment (i.e. collection of security goals)
- 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.

Introduction

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

- a detailed specification of the environment (i.e. collection of security goals)
- 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.

Introduction

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

- a detailed specification of the environment (i.e. collection of security goals)
- 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.

Introduction

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

- a detailed specification of the environment (i.e. collection of security goals)
- 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.

Introduction

Cryptography provides our designer 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 schemes etc.

- authentication protocols
- key establishment protocols
- variety of application oriented protocols
  - electronic payment systems
  - electronic election

Introduction

Cryptography provides our designer 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 schemes etc.

- authentication protocols
- key establishment protocols
- variety of application oriented protocols
  - electronic payment systems
  - electronic election

Introduction

Cryptography provides our designer 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 schemes etc.

- authentication protocols
- key establishment protocols
- variety of application oriented protocols
  - electronic payment systems
  - electronic election

Introduction

Cryptography provides our designer 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 schemes etc.

- authentication protocols
- key establishment protocols
- variety of application oriented protocols
  - electronic payment systems
  - electronic election

Introduction

Cryptography provides our designer 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 schemes etc.

- authentication protocols
- key establishment protocols
- variety of application oriented protocols
  - electronic payment systems
  - electronic election

Introduction

Cryptography provides our designer 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 schemes etc.

More complex tools and services:

- authentication protocols
- key establishment protocols
- variety of application oriented protocols
  - electronic payment systems
  - electronic election

Introduction

Cryptography provides our designer 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 schemes etc.

More complex tools and services:

- authentication protocols
- key establishment protocols
- variety of application oriented protocols
  - electronic payment systems
  - electronic election

Introduction

Cryptography provides our designer 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 schemes etc.

More complex tools and services:

- authentication protocols
- key establishment protocols
- variety of application oriented protocols
  - electronic payment systems
  - electronic election

Table of Contents

Terminology

Basic security requirements:

- Confidentiality/Secrecy
- Authenticity
- Integrity
- Non-repudiation

Terminology

Basic security requirements:

- Confidentiality/Secrecy
- Authenticity
- Integrity
- Non-repudiation

Terminology

Basic security requirements:

- Confidentiality/Secrecy
- Authenticity
- Integrity
- Non-repudiation

Terminology

Basic security requirements:

- Confidentiality/Secrecy
- Authenticity
- Integrity
- Non-repudiation

Terminology

- message/plaintext
- Encryption (first cryptographic operation used to ensure secrecy)
- cryptogram/ciphertext
- Decryption
- Encryption/Decryption algorithm
- ciphers/cryptoalgorithms/cryptosystems

Terminology

- message/plaintext
- Encryption (first cryptographic operation used to ensure secrecy)
- cryptogram/ciphertext
- Decryption
- Encryption/Decryption algorithm
- ciphers/cryptoalgorithms/cryptosystems

Terminology

- message/plaintext
- Encryption (first cryptographic operation used to ensure secrecy)
- cryptogram/ciphertext
- Decryption
- Encryption/Decryption algorithm
- ciphers/cryptoalgorithms/cryptosystems

Terminology

- message/plaintext
- Encryption (first cryptographic operation used to ensure secrecy)
- cryptogram/ciphertext
- Decryption
- Encryption/Decryption algorithm
- ciphers/cryptoalgorithms/cryptosystems

Terminology

- message/plaintext
- Encryption (first cryptographic operation used to ensure secrecy)
- cryptogram/ciphertext
- Decryption
- Encryption/Decryption algorithm
- ciphers/cryptoalgorithms/cryptosystems

Terminology

- message/plaintext
- Encryption (first cryptographic operation used to ensure secrecy)
- cryptogram/ciphertext
- Decryption
- Encryption/Decryption algorithm
- ciphers/cryptoalgorithms/cryptosystems

Terminology

- Private-key or symmetric cryptosystems
- Public-key or asymmetric cryptosystems
- Hashing
- One-way functions
- Electronic signature
- Secret sharing

Terminology

- Private-key or symmetric cryptosystems
- Public-key or asymmetric cryptosystems
- Hashing
- One-way functions
- Electronic signature
- Secret sharing

Terminology

- Private-key or symmetric cryptosystems
- Public-key or asymmetric cryptosystems
- Hashing
- One-way functions
- Electronic signature
- Secret sharing

Terminology

- Private-key or symmetric cryptosystems
- Public-key or asymmetric cryptosystems
- Hashing
- One-way functions
- Electronic signature
- Secret sharing

Terminology

- Private-key or symmetric cryptosystems
- Public-key or asymmetric cryptosystems
- Hashing
- One-way functions
- Electronic signature
- Secret sharing

Terminology

- Private-key or symmetric cryptosystems
- Public-key or asymmetric cryptosystems
- Hashing
- One-way functions
- Electronic signature
- Secret sharing

Terminology

Cryptanalysis has its own terminology as well.

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

Terminology

Cryptanalysis has its own terminology as well.

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

Terminology

Cryptanalysis has its own terminology as well.

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

Terminology

Cryptanalysis has its own terminology as well.

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

Terminology

Encryption algorithm can be analysed using the following typical attacks:

- Ciphertext-only attack
- Known-plaintext attack
- Chosen-plaintext attack
- Chosen-ciphertext attack

Terminology

Encryption algorithm can be analysed using the following typical attacks:

- Ciphertext-only attack
- Known-plaintext attack
- Chosen-plaintext attack
- Chosen-ciphertext attack

Terminology

Encryption algorithm can be analysed using the following typical attacks:

- Ciphertext-only attack
- Known-plaintext attack
- Chosen-plaintext attack
- Chosen-ciphertext attack

Terminology

Encryption algorithm can be analysed using the following typical attacks:

- Ciphertext-only attack
- Known-plaintext attack
- Chosen-plaintext attack
- Chosen-ciphertext attack

Terminology

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

- Impersonation attack
- Substitution attack
- Spoofing attack
- collision
- birthday attack
- pseudo-collision

Terminology

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

- Impersonation attack
- Substitution attack
- Spoofing attack
- collision
- birthday attack
- pseudo-collision

Terminology

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

- Impersonation attack
- Substitution attack
- Spoofing attack

- collision
- birthday attack
- pseudo-collision

Terminology

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

Terminology

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

Terminology

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