Cryptography Concepts and Terminology

Cryptography

School of Engineering and Technology
CQUniversity Australia

Prepared by Steven Gordon on 04 Jan 2022,
concepts.tex, r1961

Contents

Important Security Protections

Confidentiality ensures only authorised parties can view information

Integrity ensures information, including identity of sender, is not altered

Availability ensures information accessible to authorised parties when needed

Examples of confidentiality: a file is encrypted so that only authorised party (with a secret key) can decrypt to read the contents of the file; web traffic sent across Internet is encrypted so that intermediate users cannot see the web sites and content of web pages you are visiting.

Examples of integrity: If someone maliciously modifies a message, the receiver can detect that modification; if someone sends a message pretending to be someone else, the receiver can detect that it is a different person.

Examples of availability: a web server provides customers ability to buy products; that web server is available for the customers 24/7 even under malicious attacks.

Other Common Protections

Authentication ensures that the individual is who she claims to be (the authentic or genuine person) and not an impostor

Authorisation providing permission or approval to use specific technology resources

Accounting provides tracking of events

Example of authentication: check username and password when user logs into system.

Example of authorisation: check that user is authorised to access a particular document.

Example of accounting: record logs of who accesses files and provide summary reports.

Scope

- Focus on confidentiality and integrity of information using technical means
- Means of authentication also covered
- Accounting, system availability, policy, etc. are out of scope
- See other subjects or books on “IT Security”, “Network Security Concepts” or similar

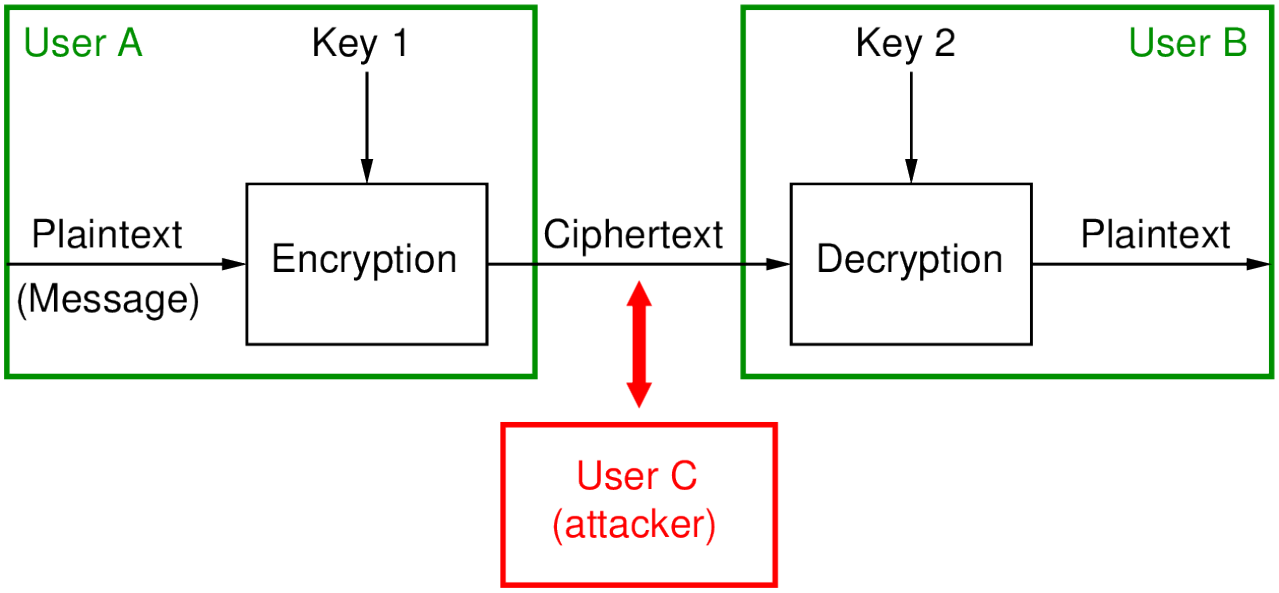
Contents

Encryption for Confidentiality

- Aim: assure confidential information not made available to unauthorised individuals (data confidentiality)
- How: encrypt the original data; anyone can see the encrypted data, but only authorised individuals can decrypt to see the original data
- Used for both sending data across network and storing data on a computer system

While encryption is used to provide different services in cryptography, the main service is confidentiality: keeping data secret. In the following we talk about using encryption for confidentiality. Later we will see that the same encryption mechanisms can also provide other services such as authentication, integrity and digital signatures.

Model of Encryption for Confidentiality



The figure on slide 8 shows a simple model of system that uses encryption for confidentiality. Assume two users, A and B, want to communicate confidentially. User A has a plaintext message to send to B. User A first encrypts that plaintext using a key. The output ciphertext is sent to user B (e.g. across the Internet). We assume the attacker, user C, can intercept anything sent – in this case they see the ciphertext. User B receives the ciphertext and decrypts. If the correct key and algorithm is used, then the output of the decryption is the original plaintext.

The aim of the attacker is to find the plaintext. They can either do some analysis of the ciphertext to try to discover the plaintext, or try to find the key (if the attacker knows key 2, they can decrypt the same as user B).

In symmetric key crypto, Key 1 and Key 2 are identical (symmetry of the keys).

In public key crypto, Key 1 is the public key of B and Key 2 is the private key of B. (asymmetric of the keys).

Cryptography Terms

Plaintext original message

Ciphertext encrypted or coded message

Encryption convert from plaintext to ciphertext (enciphering)

Decryption restore the plaintext from ciphertext (deciphering)

Key information used in cipher known only to sender/receiver

Cipher a particular algorithm (cryptographic system)

Cryptography study of algorithms used for encryption

Cryptanalysis study of techniques for decryption without knowledge of plaintext

Cryptology areas of cryptography and cryptanalysis

Contents

Common Symbols and Notation

Symbol	*Description*	*Example*
P	Plaintext or message	$P = \mathrm{D}(K_{AB}, C)$
M	Message or plaintext	$M = \mathrm{D}(PR_B, C)$
C	Ciphertext	$C = \mathrm{E}(K_{AB}, P)$ or $C = \mathrm{E}(PU_B, M)$
K	Secret key, symmetric key	
K_{AB}	Secret key shared between A and B	
E()	Encrypt operation	$\mathrm{E}(K_{AB}, P)$ or $\mathrm{E}(PU_B, M)$
$\mathrm{E}_{cipher}()$	Encrypt operation using cipher	$\mathrm{E}_{AES}(K_{AB}, P)$
D()	Decrypt operation	$\mathrm{D}(K_{AB}, C)$ or $\mathrm{D}(PR_B, C)$
PU_A	Public key of user A	
PR_A	Private key of user A	
H()	Hash operation	$\mathrm{H}(M)$
MAC()	MAC operation	$\mathrm{MAC}(K_{AB}, M)$
XOR, $\oplus$	Exclusive OR operation	A XOR B, $A \oplus B$
h	Hash value	$h = \mathrm{H}(M)$
$\|\|$	Concatenate (join) operation	$A \| \| B$