Cryptography Concepts and Terminology

Cryptography

School of Engineering and Technology
CQUniversity Australia

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

Contents

Security Concepts

Cryptography Concepts

Cryptography Notation and Terminology

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

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

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

Security Concepts

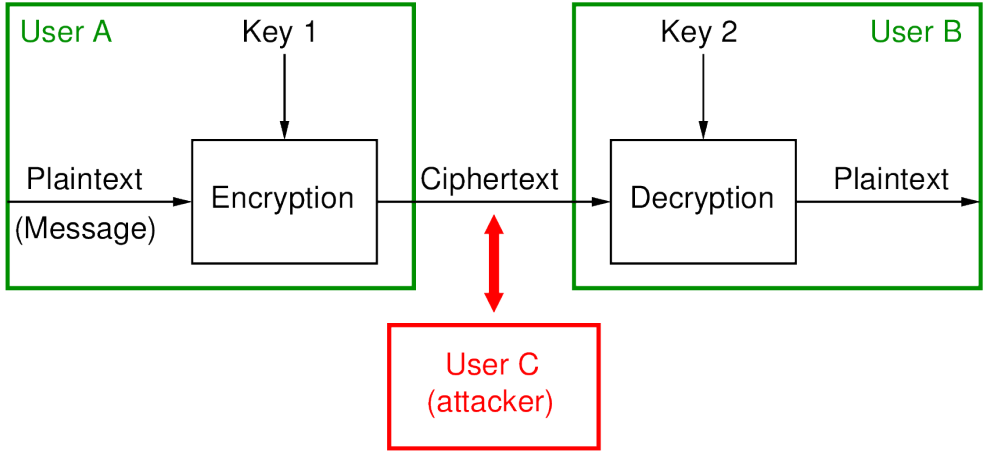
Cryptography Concepts

Cryptography Notation and Terminology

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

Model of Encryption for Confidentiality



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

Security Concepts

Cryptography Concepts

Cryptography Notation and Terminology

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	$A \| \| B$