

Cryptography and Communication Security

Abstract

A short introduction to cryptography and its applications for communication security.

Cryptography

- Cryptology, cryptography, cryptoanalysis
- κρυπτος = hidden γραφη = writing
- First examples in ancient history
 - ◆ Ceasar's Cipher reported by Suetonius
- Coding Theory
 - ◆ data compression, secrecy, error correction

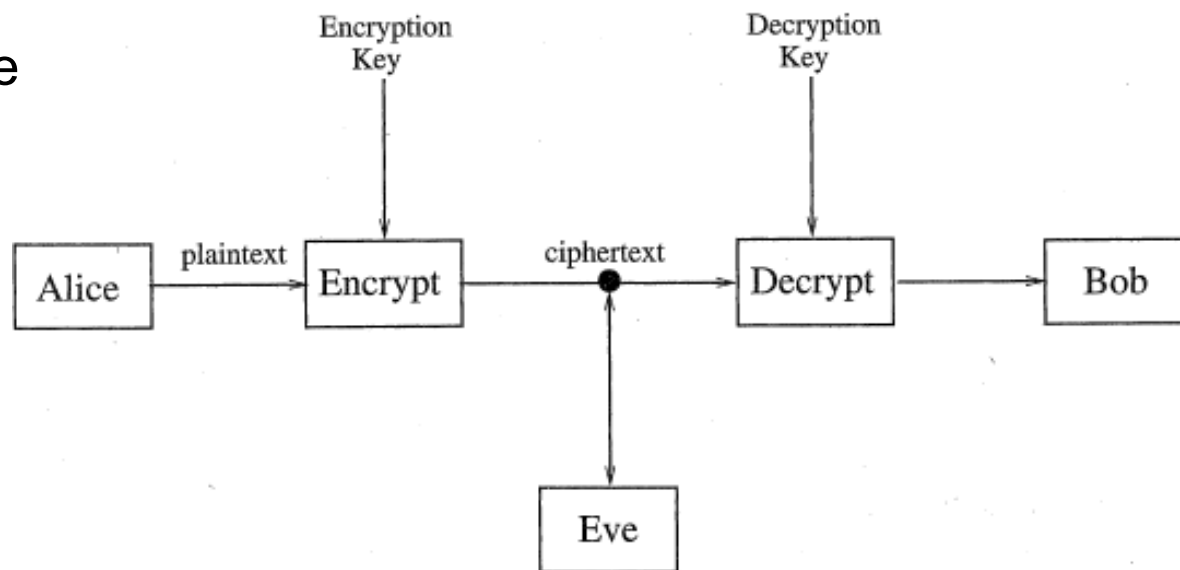
Secure Communication

- Alice sends a message to Bob using encryption
- Eve is the eavesdropper
 - ♦ active role: *Trudy, Mallory*
 - ♦ passive role: *Oscar*



Secure Communication

- Alice sends a message to Bob using encryption
- Eve may have various goals
 - read the message of Alice
 - find the key (and thus read all messages encrypted with that key)
 - corrupt the message into another message in such a way that Bob will think Alice sent the altered message
 - masquerade as Alice and thus communicate with Bob even though he believes he is communicating with Alice



Possible Attacks

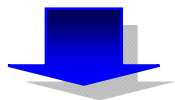
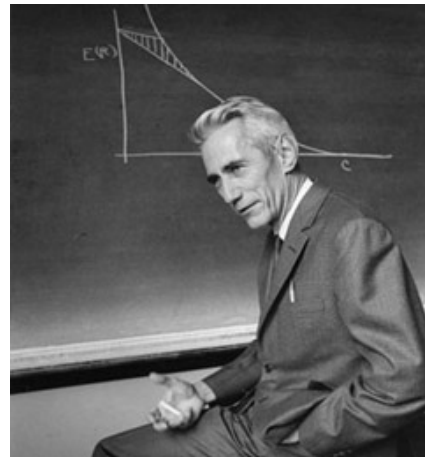
- Ciphertext only
 - ◆ Eve has only a copy of the ciphertext
- Known plaintext
 - ◆ Eve has a copy of the ciphertext and the corresponding plaintext
- Chosen plaintext
 - ◆ Eve gains temporary access to the encryption machine and uses it on several samples of plaintext
- Chosen ciphertext
 - ◆ Eve gains temporary access to the decryption machine and uses it on several samples of ciphertext

Kerckhoffs's Principle

- ***Always assume that the enemy knows the method that is being used***
(Auguste Kerckhoffs, *La Cryptographie Militaire*, 1883)



- Claude E. Shannon:
the enemy knows the system



- That is, **the security of the communication system is based on keeping secret the key, not the method**

Historic Progression of Cryptography

- Earliest years
 - ◆ security depended on the secrecy of the encryption method and the key (e.g., Ceasar's Cipher)
- Later on: *symmetric key cryptography*
 - ◆ the method is assumed known
 - ◆ security depends on the secrecy of the symmetric encryption key(s)
- Next step: *public key cryptography*
 - ◆ both the encryption method and the encryption key are made public
 - ◆ everyone knows what has to be done to find the decryption key
 - ◆ security is based on the fact that finding the decryption key from the public information is *computationally* unfeasible



Symmetric vs. Public Key Encryption

- Symmetric key encryption algorithms
 - ◆ both encryption and decryption keys are known by both and only Alice and Bob
 - ◆ examples: all traditional ciphers, DES, AES
 - ◆ key issue: [communicating the keys securely](#)
- Public key encryption algorithms
 - ◆ the encryption key is public, but the decryption key is known only by the intended recipient
 - ◆ algorithms developed since the '70s, although the principle was conceived before (free locks for everyone!)
 - ◆ examples: RSA, El Gamal, NTRU, McEliece
 - ◆ key issue: [trusting that a public key is really posted by the intended recipient](#)

How Big is a Big Number?

■ $2^n = 10^k$ with $n = k \cdot \log_2 10$ ($\log_2 10 = \sim 3.322 = \sim 1/0.301$)

◆ $2^{10} = \sim 10^3$

◆ $2^{16} = \sim 6.6 \cdot 10^4$

◆ $2^{30} = \sim 1.1 \cdot 10^9$

◆ $2^{32} = \sim 4.3 \cdot 10^9$

← 10^{11} number of stars in our galaxy

◆ $2^{48} = \sim 2.8 \cdot 10^{14}$

◆ $2^{56} = \sim 7.2 \cdot 10^{16}$

◆ $2^{60} = \sim 1.2 \cdot 10^{18}$

◆ $2^{64} = \sim 1.8 \cdot 10^{19}$

← 10^{23} Avogadro constant

◆ $2^{100} = \sim 1.3 \cdot 10^{30}$

← 10^{33} mass of the Sun [g]

◆ $2^{128} = \sim 3.4 \cdot 10^{38}$

◆ $2^{256} = \sim 1.2 \cdot 10^{77}$

← 10^{78} number of protons in the observable universe

◆ $2^{512} = \sim 1.3 \cdot 10^{154}$

← 10^{100} Googol

◆ $2^{1024} = \sim 1.8 \cdot 10^{308}$

◆ $2^{2048} = \sim 3.2 \cdot 10^{616}$

← $10^{\text{Googol}} = 10^{10^{100}}$ Googolplex

Brute Force Attack

- Trying all possible keys until the correct value is found

- Examples

<i>bits</i>	<i>keys</i>	<i>time to try all keys (1 ns / key)</i>	
♦ 32	$2^{32} = \sim 4.3 \cdot 10^9$	4 s	
♦ 56	$2^{56} = \sim 7.2 \cdot 10^{16}$	27 months	
♦ 64	$2^{64} = \sim 1.8 \cdot 10^{19}$	593 years	
♦ 128	$2^{128} = \sim 3.4 \cdot 10^{38}$	10^{22} years	← 10^{10} years: age of universe
♦ 256	$2^{256} = \sim 1.2 \cdot 10^{77}$	10^{60} years	
♦ 512	$2^{512} = \sim 1.3 \cdot 10^{154}$	10^{137} years	



Applications of Cryptography

- Main goals
 - ◆ confidentiality
 - ◆ data integrity
 - ◆ authentication (of an entity or of data origin)
 - ◆ non-repudiation
- Applications of Cryptography beyond data encryption
 - ◆ digital signature
 - ◆ identification (entity authentication)
 - ◆ message authentication
 - ◆ key establishment
 - ◆ secret sharing
 - ◆ security protocols
 - ◆ digital currency
 - ◆ games