

History of Cryptography

- Mesopotamia: encrypt recipes
- Greece: permutation cipher
- Romans: Caesar substitution cipher

⇒ SPN ciphers

Substitution Permutation Network

- 9th century: Al-Kindi (how to attack polyalphabetic ciphers)

WWII: mechanical ciphers

- enigma machine (Germany)

Alan Turing

- chosen plain text attack

Modern Cryptography

- Claude Shannon's work on information theoretic security
- Invention of public key cryptography (1976)
- Ad-hoc crypto ⇒ Provable crypto

"If computing discrete logs is hard,
then El Gamal is a secure crypto system"

system: SSH, PGP, Linux

CSE 508, 509

protocols: RSA encryption, CBC-mode

← this class

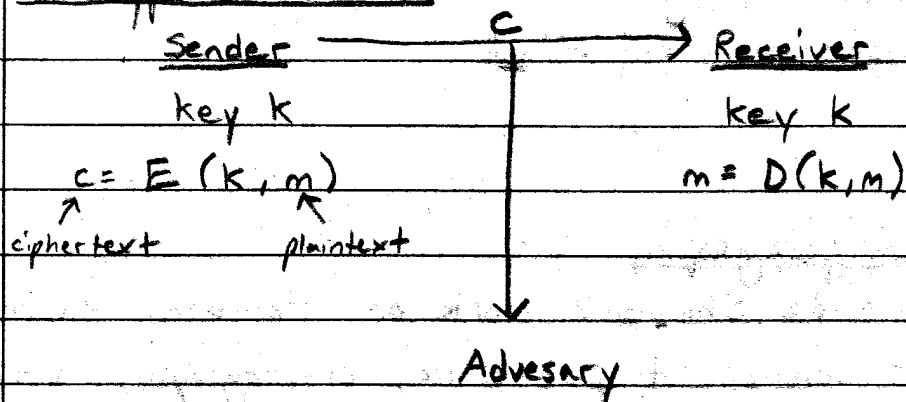
primitives: multiplication, AES

← maybe

Goals of Cryptography

- message confidentiality (secrecy)
- secure deletion
- message integrity/authenticity
- random number generation
- user authentication
- key exchange
- electronic voting
- digital cash

Encryption Schemes



Def.: An encryption scheme is a triple (G, E, D) of randomized functions

$G: \phi \rightarrow \text{keys}$

$E: \text{keys} \times \mathcal{M} \rightarrow \mathcal{C}$

$D: \text{keys} \times \mathcal{C} \rightarrow \mathcal{M}$

s.t. $D(K, E(K, m)) = m \quad \forall m, k$

The One-Time Pad

$\text{keys} = \mathcal{M}, \mathcal{C} = \{0, 1\}^l$ (l -bit strings)

$E(k, m) = k \oplus m$

$D(k, c) = k \oplus c$

$D(k, E(k, m)) = k \oplus (k \oplus m)$

$= (k \oplus k) \oplus m$

$= 0 \oplus m$

$= m$

Key re-use attack

adversary sees $\begin{cases} c_1 = k \oplus m_1 \\ c_2 = k \oplus m_2 \end{cases}$

$c_1 \oplus c_2 = k \oplus k \oplus m_1 \oplus m_2$
 $= m_1 \oplus m_2$

$m_1 = 1001101100111$

$m_2 = 001101100111$

$t = m_1 \oplus m_2 = 101011010100$

Adversary guesses $m_1[0] = 1$

$+ [0] = m_1[0] \oplus m_2[0] = m_1[0] \oplus m_1[1] = 1 \oplus m_1[1]$
 $\Rightarrow m_1[1] = 0$

Information Theoretic Security

Intuition: Knowing the ciphertext tells the attacker nothing \therefore

Def.: (Perfect Secrecy)

An encryption scheme has perfect secrecy if

$$Pr_K [E(K, m) = c]$$

$$= Pr_K [E(K, m_0) = c]$$

$$\forall m, m_0, c$$

Thm.: The one-time pad offers perfect secrecy