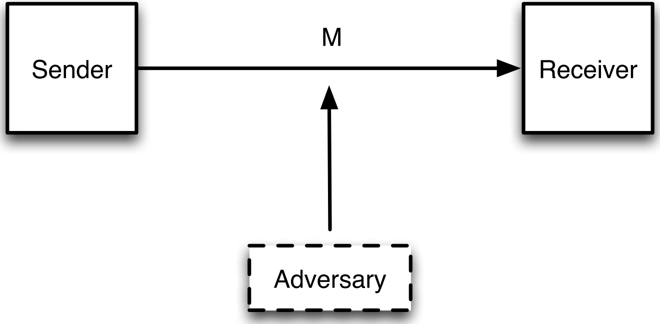
Public-Key Cryptography

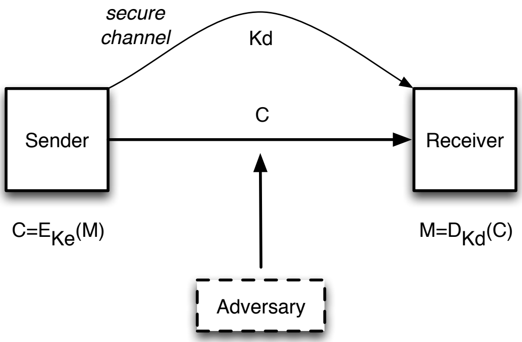
Çetin Kaya Koç

koc@cs.ucsb.edu

Secure Communication over an Insecure Channel



Secret-Key Cryptography



Encryption and decryption functions: $E(\cdot)$ & $D(\cdot)$
Encryption and decryption keys: K_e & K_d
Plaintext and ciphertext: M & C

Secret-Key Cryptography

- $C = E_{K_e}(M)$ and $M = D_{K_d}(C)$
- $\boxed{\text{Either}}$ $E(\cdot) = D(\cdot)$ and $K_e \neq K_d$

  K_d is easily deduced from K_e
  K_e is easily deduced from K_d
- $\boxed{\text{Or}}$ $E(\cdot) \neq D(\cdot)$ and $K_e = K_d$

  $D(\cdot)$ is easily deduced from $E(\cdot)$
  $E(\cdot)$ is easily deduced from $D(\cdot)$

Example: Hill Algebra

- Encoding: $\{a, b, \ldots, z\} \longrightarrow \{0, 1, \ldots, 25\}$
- Select a $d \times d$ matrix $\mathcal{A}$ of integers and find its inverse $\mathcal{A}^{-1}$ mod 26
- For example, for $d = 2$

$$\mathcal{A} = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \quad \text{and} \quad \mathcal{A}^{-1} = \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}$$

Verify:

$$\begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} = \begin{bmatrix} 105 & 78 \\ 130 & 79 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{26}$$

Hill Cipher

- Encryption function: $c = E(m) = \mathcal{A}\, m \pmod{26}$
- Decryption function: $m = D(c) = \mathcal{A}^{-1}\, c \pmod{26}$
- m and c are $d \times 1$ vectors of plaintext and ciphertext letter encodings
- Encryption key K_e: $\mathcal{A}$
- Decryption key K_d: $\mathcal{A}^{-1} \pmod{26}$
- $\mathcal{A}$ and $\mathcal{A}^{-1}$ are $d \times d$ matrices such that $\det(\mathcal{A}) \neq 0 \pmod{26}$ and $\mathcal{A}^{-1}$ is the inverse of $\mathcal{A}$ mod 26

Secret-Key versus Public-Key Cryptography

- Secret-Key Cryptography:
  - Requires establishment of a secure channel for key exchange
  - Two parties cannot start communication if they never met
  - Secure communication of n parties requires $n(n-1)/2$ keys
  - Keys are "shared", rather than "owned" (secret vs private)
- Public-Key Cryptography:
  - No need for a secure channel
  - May require establishment of a public-key directory
  - Two parties can start communication even if they never met
  - Secure communication of n parties requires n keys
  - Keys are "owned', rather than "shared"
  - Ability to "sign" digital data (secret vs private)

Diffie-Hellman Key Exchange Method

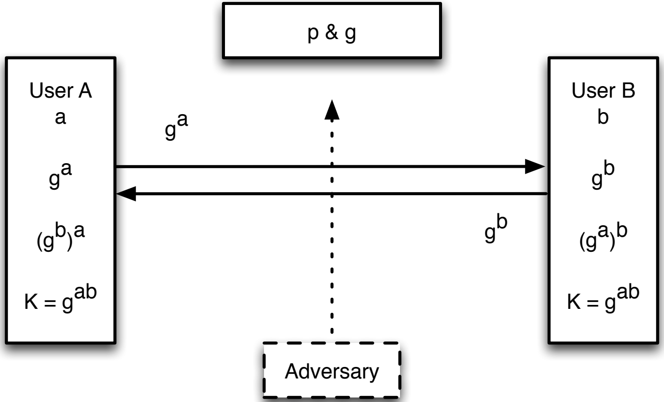
- Martin Hellman (1945): American cryptologist and co-inventor of public key cryptography in cooperation with Whitfield Diffie and Ralph Merkle at Stanford
- Bailey Whitfield Diffie (1944) is an American cryptographer and co-inventor of public key cryptography
- Diffie and Hellman's paper "New Directions in Cryptography" was published *IEEE Tran. Information Theory* in Nov 1976
- It introduced a radically new method of distributing cryptographic keys, that went far toward solving one of the fundamental problems of cryptography, key distribution
- It has become known as Diffie-Hellman key exchange.

Diffie-Hellman Key Exchange Method

- A and B agree on a prime p and a primitive element g of $\mathcal{Z}_p^*$
- This is accomplished in public: p and g are known to the adversary
- A selects $a \in \mathcal{Z}_p^*$, computes $s = g^a \pmod{p}$, and sends s to B
- B selects $b \in \mathcal{Z}_p^*$, computes $r = g^b \pmod{p}$, and sends r to A
- A computes $K = r^a \pmod{p}$
- B computes $K = s^b \pmod{p}$

$$K = r^a = (g^b)^a = g^{ab} \pmod{p}$$
$$K = s^b = (g^a)^b = g^{ab} \pmod{p}$$

Diffie-Hellman Key Exchange Method



Discrete Logarithm Problem

- The adversary knows the group: p and g
- The adversary also sees (obtains copies of) $s = g^a$ and $r = g^b$
- The **discrete logarithm problem** (DLP):
  the computation of $x \in \mathcal{Z}_p^*$ in

$$y = g^x \pmod{p}$$

  given p, g, and y
- Example: Given $p = 23$ and $g = 5$, find x such that

$$10 = 5^x \pmod{23}$$

  Answer: $x = 3$

Discrete Logarithm Problem

- Given $p = 158(2^{800} + 25) + 1 =$

  1053546280395016975304616582933958731948871814925913489342
  6087342587178835751858673003862877377055779373829258737624
  5199045043066135085968269741025626827114728303489756321430
  0237166369174066615907176472549470083113107138189921280884
  003892629359

  and $g = 3$, find $x \in \mathcal{Z}_p^*$ such that

  $$2 = 3^x \pmod{p}$$

  Answer: ?

- How difficult is it to find x?

Diffie-Hellman Key Exchange Method

- The Diffie-Hellman algorithm allows two parties to agree on a key that is known only to them, except that the adversary can solve the DLP
- Once the secret key (shared key) is established, the parties can use a secret-key cryptographic algorithm to encrypt and decrypt
- However, we still have the problem of establishing $n(n-1)/2$ keys between n parties, and other difficulties of the secret-key cryptography also remain
- But, we no longer need a (secret-key type) secure channel — the Diffie-Hellman algorithm gave us a secure channel, whose security depends on computational difficulty of the DLP
- The Diffie-Hellman algorithm is not a public-key encryption method

Public-Key Cryptography

- The functions $C(\cdot)$ and $D(\cdot)$ are inverses of one another

$$C = E_{K_e}(M) \quad \text{and} \quad M = D_{K_d}(C)$$

- Encryption and decryption processes are **asymmetric**:

$$K_e \neq K_d$$

- K_e is **public**, known to everyone
- K_d is **private**, known only to the user
- K_e may be easily deduced from K_d
- However, K_d is **NOT easily** deduced from K_e