Symmetric-key Encryption

Dawn Song
dawnsong@cs.berkeley.edu

Cryptology

- **Cryptology is the study of Cryptography & Cryptanalysis**
- **Cryptography**
  - **Literally:**
    Crypt: secret, graphia: writing---Cryptography: the study of how to send secret messages
  - **Formally:**
    The study of mathematical techniques to enforce security properties: Confidentiality, integrity, etc.
- **Cryptanalysis is the study of how to break cryptographic systems**

Brief History of Cryptography (I)

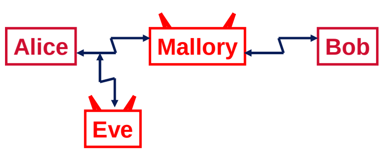
- **First phase: manual**
  - **Caesar cypher (Romans)**
    - » **Permute the alphabet by shifting each letter forward by a fixed amount**
    - » **Caesar cipher with a shift by 3:**
      - **What's the original message for "fubswrjudskb"?**
  - **Clearly not very secure**
- **Second phase: mechanical era**
  - **Enigma machine: a German project to create a mechanical encryption/decryption device**
  - **British effort to break the code**
    - » **Important for WWII, estimate shortening war by 1 year**

Brief History of Cryptography (II)

- Third phase: Modern Cryptography
  - Relying on mathematics and electronic computers
  - Early roots by Claude Shannon
    - E.g., One-time pad
  - DES by NIST (1970's)
  - ...

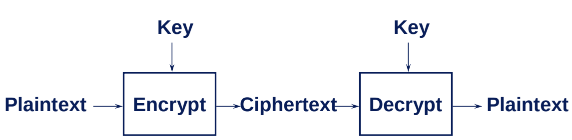
Basic Communication Setting

- Introducing security protocol participants
  - Alice (usually the protocol initiator)
  - Bob, Alice's friend
  - Eve the eavesdropper (passive attacker)
  - Mallory the malicious attacker (active attacker)
- Basic setting



Symmetric-key Model

- Encryption key = decryption key
- Encryption: E_K(plaintext) = ciphertext
- Decryption: D_K(ciphertext) = plaintext
- We write $\{\text{plaintext}\}_K$ for E_K(plaintext)



Threat Model

- **Known ciphertext (ciphertext only)**
  - **Attacker only has a copy of some ciphertext**
- **Known plaintext**
  - **Attacker obtains ciphertext and corresponding plaintext**
- **Chosen plaintext**
  - **Attacker can choose plaintext that is going to be encrypted and obtains ciphertext**
- **Chosen Ciphertext**
  - **Attacker can choose ciphertext and obtains corresponding plaintext**

One-time Pad

- **Alice & Bob share an n-bit secret key K = K1…Kn, where bits K1,…,Kn chosen randomly**
- **Alice wishes to send n-bit msg M = M1…Mn**
- **Desired properties of the encryption scheme:**
  - **Can encrypt: map M to C = C1…Cn**
  - **Given knowledge of K, easy to decrypt: get M from C**
  - **Eve, who doesn't know K, should learn no info about M**
- **Encryption scheme: $C = M \oplus K$**
  - **$Cj = Mj \oplus Kj$**

XOR Properties

- **XOR truth table**

a	b	$a \oplus b$
0	0	0
0	1	1
1	0	1
1	1	0

- **Some XOR properties**
  - **$a \oplus a = 0$**
  - **$a \oplus b \oplus b = a$**

How Secure is One-time Pad?

- What may Eve learn about M by seeing C?
- What if Eve knew something about M apriori?
  - Does Eve learn anything in addition?
- One-time pad is secure
  - Eve learns no additional info about M by seeing C
  - No matter what M is, C is a uniformly random n-bit string
- Proof
  - For a given M, any C is possible by picking the unique K: $K = M \oplus C$
  - Each such K is equally likely
  - Thus C is equally likely to be any n-bit string

Disadvantage of One-time Pad

- K needs be the same length as the message & can't be reused
- What happens if reuse K?
  - $C = M \oplus K$
  - $C' = M' \oplus K$
  - Eve learns $M \oplus M'$

Administrative Matters

- Waitlist
- Assigned reading
- Discussion sections
- Mailing list vs. newsgroup

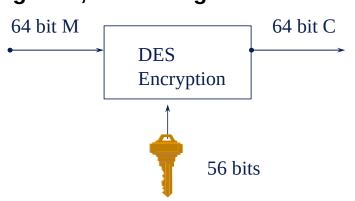
3-min Stretch Break

Block Cipher

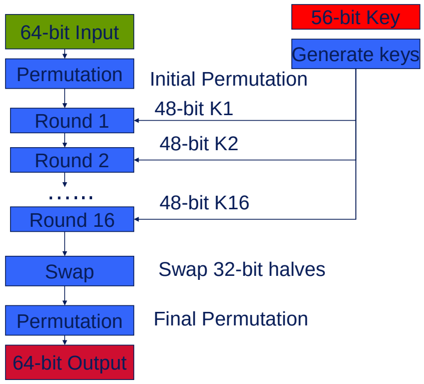
- Alice & Bob share a k-bit random key K
- Encrypt an n-bit msg M into n-bit ciphertext C
- Encryption function E:
  - C = E(K, M)
- Decryption function D:
  - M = D(K, C)

DES

- Data Encryption Standard (DES)
  - An example of a block cipher
  - Designed by IBM in 1974 responding to NIST request
  - Standardized in 1979
- Designed for fast VLSI implementation
- Key length 56, block length 64

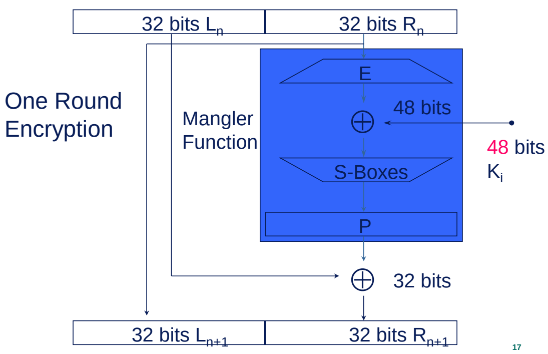


DES Overview



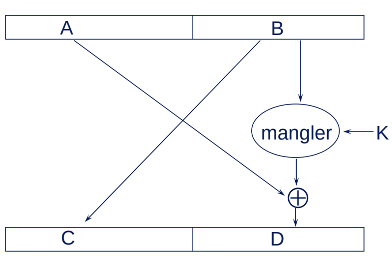
16

A DES Round



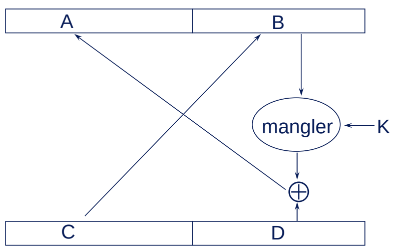
17

Feistel Cipher Encryption



18

Feistel Cipher Decryption



19

Why Feistel?

- So mangler function f doesn't need to be reversible
  - enc(A,B): C=B, D=A ⊕ f(B)
  - dec(C,D): B=C,
    A=D ⊕ f(C), because A ⊕f(B) ⊕f(B) = A
- DES is Feistel

20

How Secure is DES?

- Best practical attack known is exhaustive key search
  - 2^{55} (due to symmetry in key structure)
- 1977: Diffie & Hellman: $20,000,000 machine that breaks DES key in 1 day
- 1993: Wiener: $100,000 machine that breaks DES key in 1.5 days
- 1998: EFF's DES Cracker
  - EFF spent $250,000 to build it
  - Tests $88*10^9$ keys per second
  - Solved DES Challenge II-2 in 56 hours
- 1999: DES Cracker + distributed.net (100,000 computers)
  - Tests $254*10^9$ keys per second
  - Solved DES Challenge III in 22 hours

21

Advanced Encryption Standard AES

- 1998 NIST announced a competition for a new cipher
  - DES block length is too short
- Winning cipher was Rijndael (pronounced Rhine-doll)
  - Belgian designers: Joan Daemen & Vincent Rijmen
  - Adopted by NIST as Advanced Encryption Standard (AES), Nov 2001
- Officially adopted for US government work, but voluntarily adopted by private sector
- Block length 128, Key size: 128, 192, or 256
- AES is not Feistel
  - All functions are reversible
- High-speed cipher
  - About 16 clock cycles/byte on modern 32-bit CPUs
  - That’s 200 MByte/s on a 3.2 GHz P4!