Basic Cryptographic Functions and Some Simple Protocols

CSCI-7000-001 fall'01 (04)

Antonio Carzaniga

Outline

- Some cryptographic functions
- Introduction to cryptographic protocols

Cryptographic Function

- Function in the mathematical sense:

  ciphertext = E_k(plaintext) "encryption"

  plaintext = D_k(ciphertext) "decryption"

One-way Hash Functions

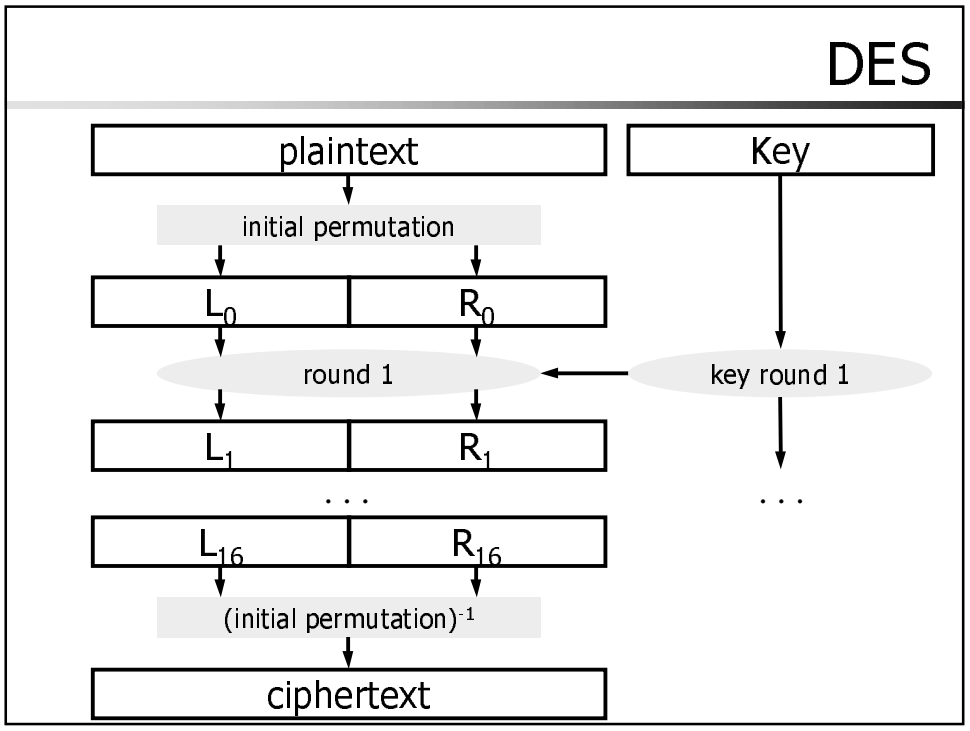
- No Keys
- One-way
  - F is efficient, F^{-1} is intractable
- Hash
  - |ciphertext| = constant (e.g., 128 bits)
  - collision-free: probability[$x \neq y \wedge H(x)=H(y)$]
    - perfect hash: P [$x \neq y \wedge H(x)=H(y)$] = $2^{-|H()|}$

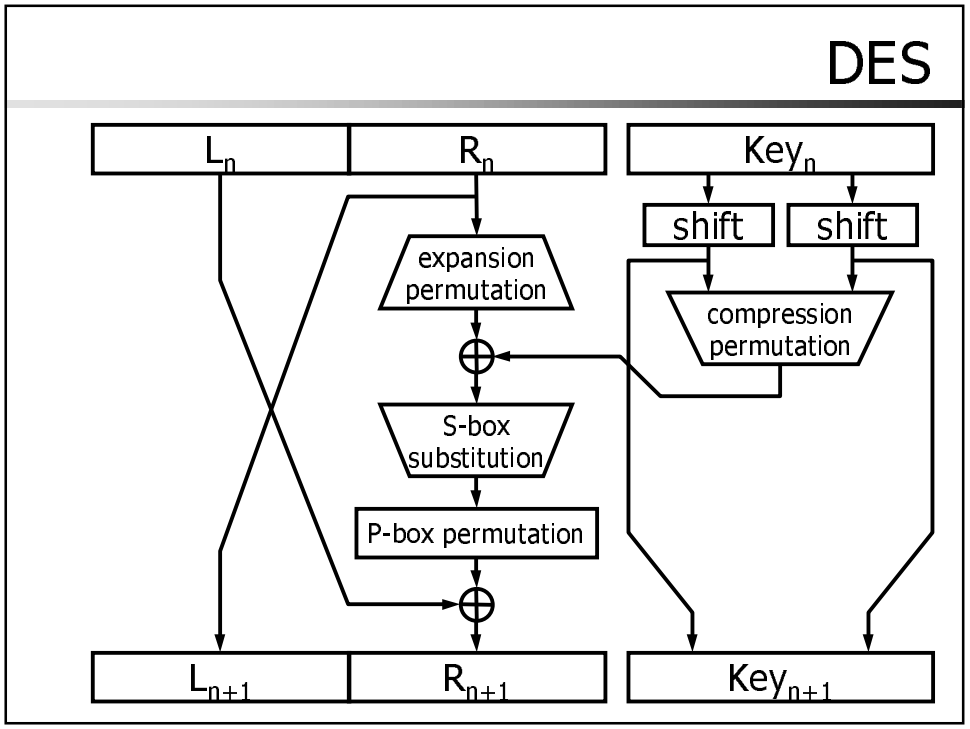
Conventional Encryption

- A.k.a. symmetric or secret-key cryptography
- designed to be reversible, i.e., $D_k=E_k^{-1}$
- 1 key, shared by E() and D()
- |ciphertext| ≅ |plaintext|
  (should be |ciphertext| ≤ |plaintext|)

Public-key Encryption

- A.k.a. asymmetric cryptography
- 2 Keys: K1, K2
- Asymmetric: $D_{K2}=E_{K1}^{-1}$
  - not necessarily $D_{K1}=E_{K1}$ (although true for RSA)


DES
plaintext
Key
initial permutation
L_0
R_0
round 1
key round 1
L_1
R_1
. . .
. . .
L_{16}
R_{16}
$(\text{initial permutation})^{-1}$
ciphertext


DES
L_n
R_n
Key_n
shift
shift
expansion permutation
compression permutation
S-box substitution
P-box permutation
L_{n+1}
R_{n+1}
Key_{n+1}

Other Conventional Ciphers

- Basic Feistel block structure
- Classification
  - algorithm
  - key length
  - number of rounds
  - classes of operations in each round

Table of Symmetric Ciphers

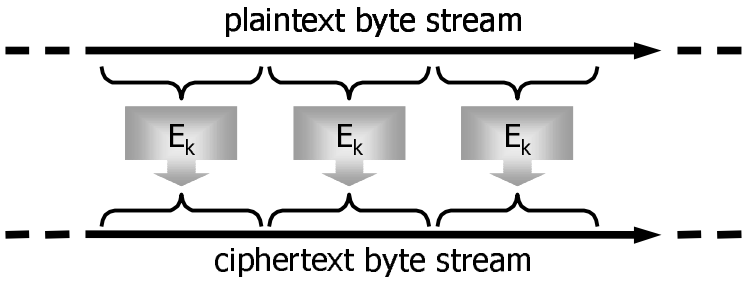
Algorithm	*Key size*	*# of rounds*	*Operations*	*Applications*
DES	56	16	XOR, fixed S-boxes	Kerberos
3DES	112 or 168	48	XOR, fixed S-boxes	Fin. Key mgmt, PGP, S/MIME
IDEA	128	8	XOR, +, *	PGP
Blowfish	Up to 448	16	XOR, var S-boxes, +	
RC5	Up to 2048	Up to 255	XOR, +, -, shift	
CAST-128	40~128	16	XOR, fixed S-boxes, +, -, shift	PGP
AES Rijndael	128, 192, 256	9, 11, 13	fixed S-boxes, shift,*,+,XOR	…

How to Use Conventional Ciphers

- Encryption of long messages (practically every message)
- Increasing security through multiple encryption

Block/Stream Ciphers

- Stream cipher: encryption/decryption one symbol (character/bit) at a time
- Block cipher: encrypt/decrypt fixed-size blocks

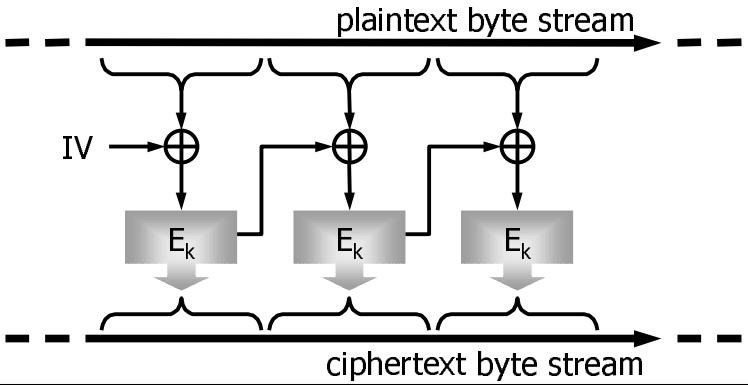


Problems of Trivial Block Ciphers

- Identical blocks of plaintext generate identical blocks of ciphertext
- Attacker can "cut&paste" ciphertext and obtain readable (edited) plaintext

Cipher Block Chaining

- Idea: mix in something random with every block
- Idea(Idea): mix in the encryption of the previous block:

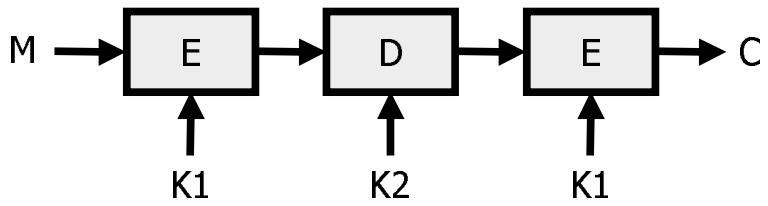


Multiple Encryption

- How to combine multiple rounds of $E_k()$ to improve security?
  - encrypting twice with same key
    $C = E_k(E_k(M))$
  - encrypting twice with two keys
    $C = E_{k1}(E_{k2}(M))$
  - encrypting three times with...
  - ...
  - encrypting four times ...
  - ...

Multiple Encryption Schema

- 3DES:
  - two keys: K1, K2
  - schema: $C = E_{K1}(D_{K2}(E_{K1}(M)))$



Protocols

- Every party knows every step of the protocol in advance
- Every party must agree to follow the protocol
- A protocol must be unambiguous
- A protocol must be complete

Classes of Protocols

- Arbitrated
- Adjudicated
- Self-enforcing

Classes of Attacks

- Passive attacks
  - attacker does not take part in the protocol
  - attacker can only observe
- Active attacks

- Cheaters: attacker is a legitimate player
  - passive
  - active

Cryptographic Protocols

- Authentication
- Key exchange
- Authentication and key exchange
- Secret splitting and sharing
- Undeniable digital signatures
- Certification
- Subliminal channel
- Proxy signature
- Group signature

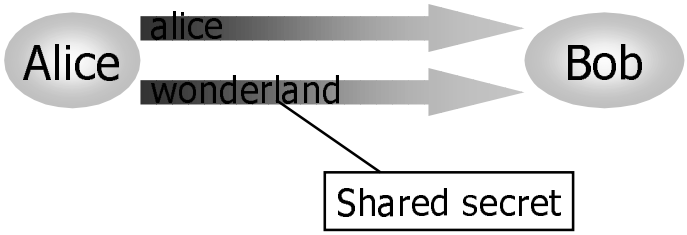
More Cryptographic Protocols

- Computing on encrypted data
- Prediction commitment
- Fair coin flip
- Mental poker
- Key escrow
- Zero-knowledge proof
- Simultaneous contract signing
- Digital certified mail
- Simultaneous exchange of secrets

Esoteric Protocols

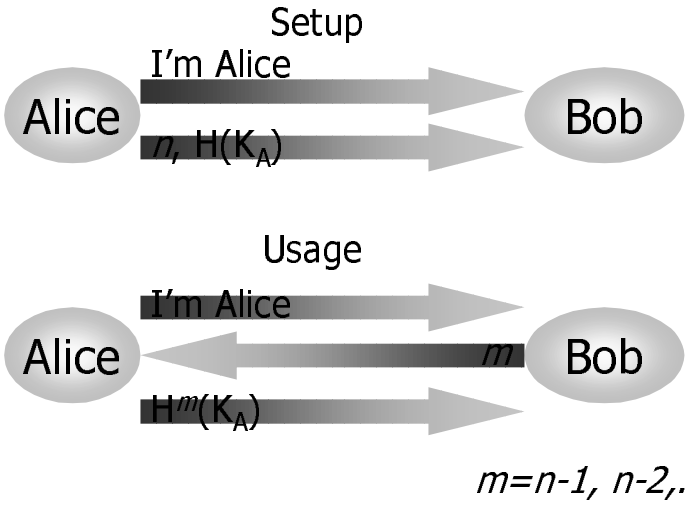
- Secure elections
- Secure multiparty computations
- Anonymous message broadcast
- Digital cash (or anonymous digital cash)

Plaintext Authentication



- Alice sends her secret password *P*
- Bob computes *H(P)* and verifies that the password is correct
- Bob does not need to store the password, it can store a hash of the password

Hash Function Authentication



Analysis of SKey

- Vulnerabilities?

  ...