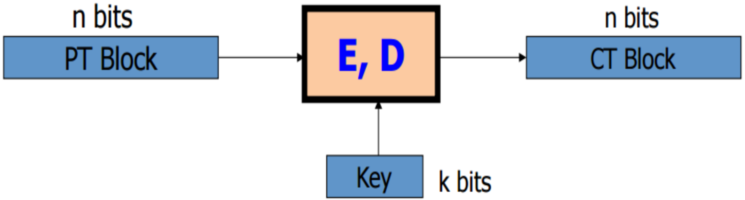
CSIT 495/595 - Introduction to Cryptography
Practical Private Key Primitives

Bharath K. Samanthula
Department of Computer Science
Montclair State University

Outline

- Block Ciphers
  - Feistel Network
  - DES
  - Triple-DES
  - AES
- Hash Functions
  - MD5
  - SHA Family: SHA-0, SHA-1, SHA-2, SHA-3

Block Ciphers



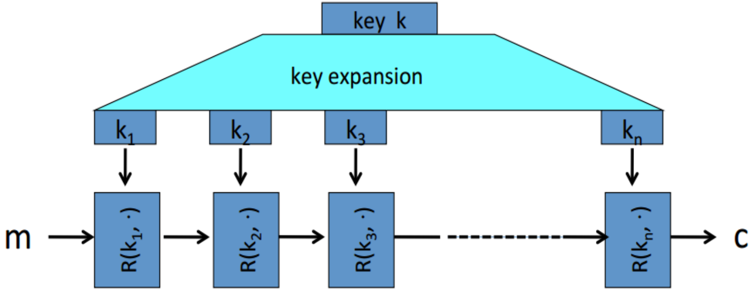
Canonical examples:

1. 3DES: n= 64 bits, k = 168 bits
2. AES: n=128 bits, k = 128, 192, 256 bits

Some slides are adopted from Block Ciphers by Dan Boneh

Block Ciphers: Iterative Approach

Most modern block ciphers are iterative in nature



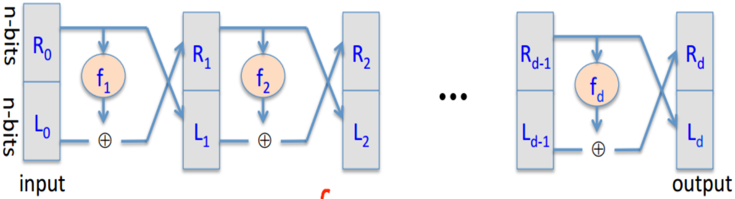
R(k,m) is called a round function

for 3DES (n=48), for AES-128 (n=10)

Feistel Network (1)

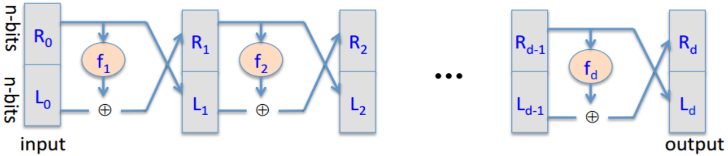
Given functions $f_1, \ldots, f_d\colon \{0,1\}^n \longrightarrow \{0,1\}^n$

Goal: build invertible function $F\colon \{0,1\}^{2n} \longrightarrow \{0,1\}^{2n}$



In symbols: $\begin{cases} R_i = f_i(R_{i-1}) \oplus L_{i-1} \\ L_i = R_{i-1} \end{cases}$

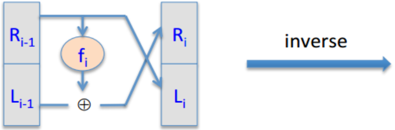
Feistel Network (2)



Claim: for all $f_1, \ldots, f_d$: $\{0,1\}^n \longrightarrow \{0,1\}^n$

Feistel network $F: \{0,1\}^{2n} \longrightarrow \{0,1\}^{2n}$ is invertible

Proof: construct inverse



$R_{i-1} = L_i$

$L_{i-1} =$???

Data Encryption Standard (DES)

- Early 1970s: Horst Feistel designs Lucifer at IBM

  key-len = 128 bits ; block-len = 128 bits

- 1973: NBS asks for block cipher proposals.

  IBM submits variant of Lucifer.

- 1976: NBS adopts DES as a federal standard

  key-len = 56 bits ; block-len = 64 bits

- 1997: DES broken by exhaustive search

- 2000: NIST adopts Rijndael as AES to replace DES

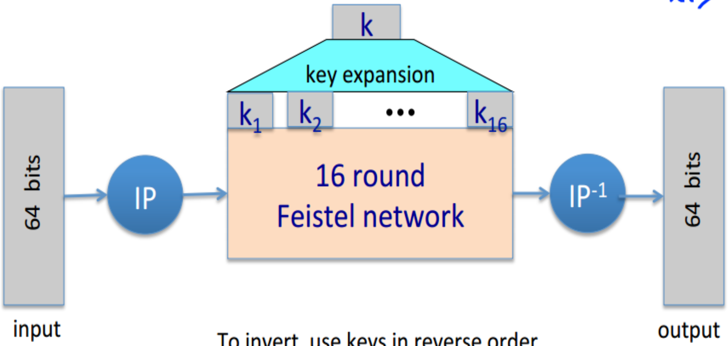
Widely deployed in banking (ACH) and commerce

DES - Graphical Interpretation

Consists of 16 rounds Feistel Network

$$f_1, \ldots, f_{16}: \{0,1\}^{32} \longrightarrow \{0,1\}^{32} \quad , \quad f_i(x) = \mathbf{F}(k_i, x)$$

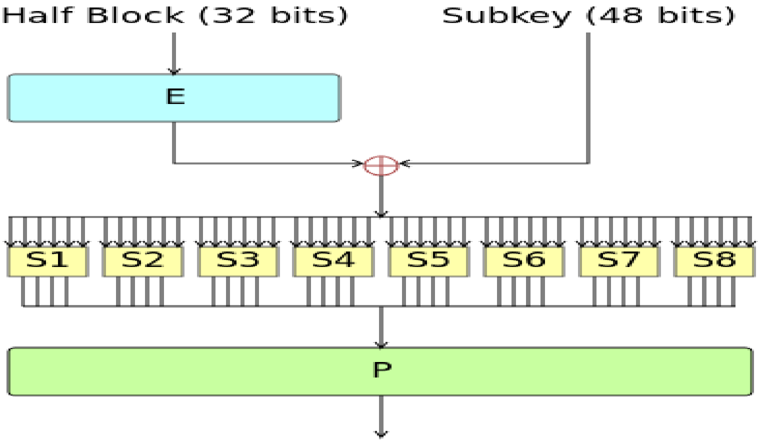
From key K



To invert, use keys in reverse order

DES - Graphical Interpretation

$F(k_i, x)$ is constructed as follows



DES - S-box Implementation

S-boxes are implemented as look-up tables

$$S_i : \{0,1\}^6 \longrightarrow \{0,1\}^4$$

S_5		Middle 4 bits of input															
		0000	**0001**	**0010**	**0011**	**0100**	**0101**	**0110**	**0111**	**1000**	**1001**	**1010**	**1011**	**1100**	**1101**	**1110**	**1111**
Outer bits	**00**	0010	1100	0100	0001	0111	1010	1011	0110	1000	0101	0011	1111	1101	0000	1110	1001
	01	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1010	0011	1001	1000	0110
	10	0100	0010	0001	1011	1010	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000	1110
	11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1010	0100	0101	0011

DES - Disadvantages

The best known attack on DES is an exhaustive search through its key space

msg = "`The unknown messages is:` XXXX ... "

CT = c_1 c_2 c_3 c_4

Goal: find $k \in \{0,1\}^{56}$ s.t. $DES(k, m_i) = c_i$ for $i=1,2,3$

1997: Internet search -- **3 months**

1998: EFF machine (deep crack) -- **3 days** (250K \$)

1999: combined search -- **22 hours**

2006: COPACOBANA (120 FPGAs) -- **7 days** (10K \$)

⇒ 56-bit ciphers should not be used !! (128-bit key ⇒ 2^{72} days)

Variants of DES

- Modification of Internal Structure – NOT Recommended
- Double DES (2DES) - Double invocation of DES
  - $E'_{k_1,k_2}(m) = E_{k_2}(E_{k_1}(m))$, where E denotes DES encryption
- Key question: Can we use 2DES to improve on the brute-force attacks of DES?
  - NO – It is susceptible to “meet-in-the-middle attack”

Triple-DES (3DES)

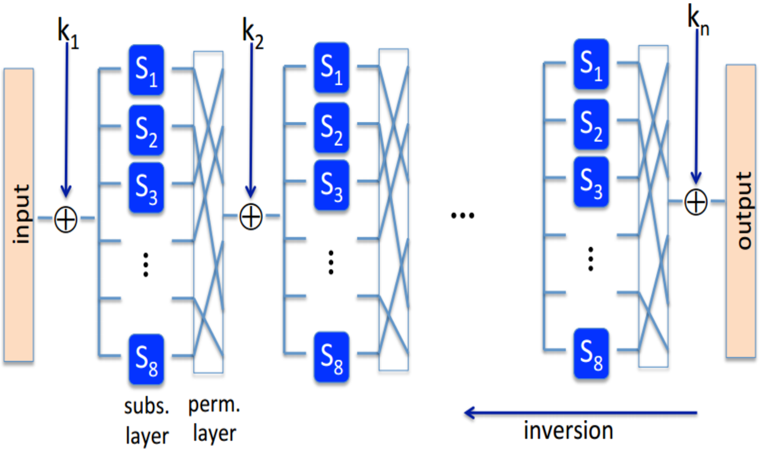
- Triple invocation of DES
  - $E'_{k_1,k_2,k_3}(m) = E_{k_3}(D_{k_2}(E_{k_1}(m)))$
  - Why do we need decryption inside the functionality?
- Standardized in 1999
- Key size: $3x56 = 168$ bits
- 3 times slower than DES

Advanced Encryption Standard (AES)

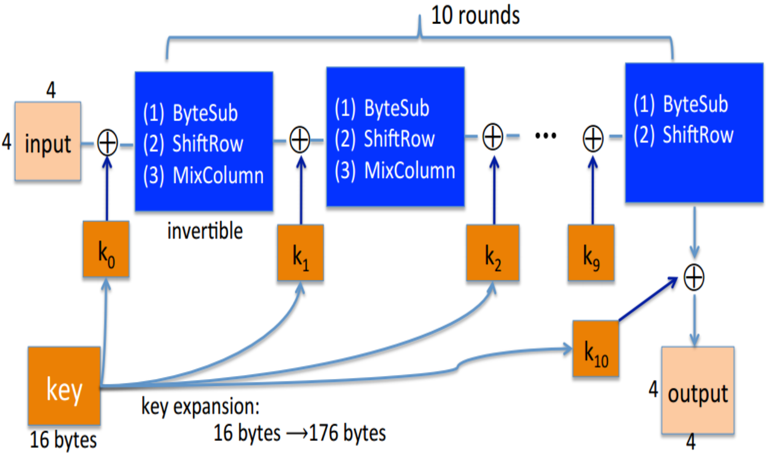
- 1997 - NIST requested for proposals to replace DES
- 1998 - 15 different algorithms were submitted
- 1999 - NIST selected 5 finalists
- October 2000 - NIST announced the winning algorithm, referred to as Rijndael, later standardized as AES
- Key sizes: 128, 192, 256 bits
- Block size: 128 bits

AES

AES is based on substitution permutation network (not Feistel)

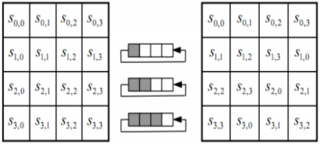


AES-128: Basic Steps

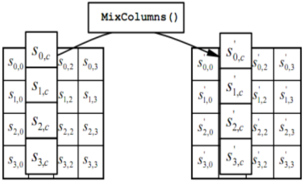


AES: The Round Function

- **ByteSub:** a 1 byte S-box. 256 byte table (easily computable)
- **ShiftRows:**



- **MixColumns:**



AES in Hardware

AES instructions in Intel Westmere:

- **aesenc, aesenclast**: do one round of AES

  128-bit registers: xmm1=state, xmm2=round key

  aesenc xmm1, xmm2 ; puts result in xmm1

- **aeskeygenassist**: performs AES key expansion

- Claim 14 x speed-up over OpenSSL on same hardware

Similar instructions on AMD Bulldozer

Practical Hash Functions

- Key requirement: hash function should be collision resistant
- Two-step construction
  1. compression function h (handles fixed-length inputs) is designed
  2. extend h to handle arbitrary input lengths
- Step 2 can be achieved using Merkle-Damgard transform
- How to achieve Step 1??

Davies-Meyer Construction

- Construct compression function from the block cipher
- Let F be a block cipher with n-bit key length and ℓ-bit block length
- The compression function $h : 0, 1^{n+\ell} \rightarrow 0, 1^{\ell}$ is defined as

$$h(k, x) = F_k(x) \oplus x$$

MD5

- A hash function with 128-bit output length (proposed in 1991)
- Considered to be collision resistant for some time
- In 2004, a group of Chinese cryptanalysts presented a method to find collisions in MD5
- Nowadays, collisions can be found in MD5 very easily (under one minute on a Desktop PC)
- Although MD5 is still being found in Legacy systems, it should not be used anywhere cryptographic security is needed

SHA Family

- A series of hash functions standardized by NIST
- SHA-0: 160 bits output length, published in 1993, but withdrawn shortly due to serious security flaws
- SHA-1: 160 bits output length, published in 1995, theoretical attack indicates that collisions can be found soon (with fewer than 2^{80} hash function evaluations)
- SHA-2: 256 or 512-bit output length, widely adopted in real-world applications

SHA-3 (Keccak)

- 2007 – NIST announced a public competition for new hash functions (51 proposals received)
- 2008 – 14 candidates were selected
- 2010 – five finalists
- October 2012 – NIST announced Keccak as the winner

Outline

- Block Ciphers
  - Feistel Network
  - DES
  - Triple-DES
  - AES
- Hash Functions
  - MD5
  - SHA Family: SHA-0, SHA-1, SHA-2, SHA-3

Useful References

- Chapter 6, Introduction to Modern Cryptography by Jonathan Katz and Yehuda Lindell, 2nd Edition, CRC Press, 2015.
- http://blogs.msdn.com/b/ace_team/archive/2007/09/07/aes-vs-3des-block-ciphers.aspx
- http://csrc.nist.gov/groups/ST/toolkit/block_ciphers.html