Symmetric Encryption: DES and AES

Jay Daigle

Occidental College

November 8, 2018

Symmetric encryption

Symmetric encryption

- The key for encrypting and decrypting is the same

Symmetric encryption

- The key for encrypting and decrypting is the same
- Key-sharing logictics: harder to use

Symmetric encryption

- The key for encrypting and decrypting is the same
- Key-sharing logictics: harder to use
- Smaller key-sizes: 80 bit key is 80 bits of security

Symmetric encryption

- The key for encrypting and decrypting is the same
- Key-sharing logictics: harder to use
- Smaller key-sizes: 80 bit key is 80 bits of security
- *Much* faster

Basic Approach

Basic Approach

Block ciphers: divide message into blocks of fixed size.

Basic Approach

Block ciphers: divide message into blocks of fixed size.

Algorithm Outline

Basic Approach

Block ciphers: divide message into blocks of fixed size.

Algorithm Outline

- Divide block in half

Basic Approach

Block ciphers: divide message into blocks of fixed size.

Algorithm Outline

- Divide block in half
- Transform right half

Basic Approach

Block ciphers: divide message into blocks of fixed size.

Algorithm Outline

- Divide block in half
- Transform right half
- Swap left and right halves

Basic Approach

Block ciphers: divide message into blocks of fixed size.

Algorithm Outline

- Divide block in half
- Transform right half
- Swap left and right halves
- Repeat some fixed number of times.

Basic Approach

Block ciphers: divide message into blocks of fixed size.

Algorithm Outline

- Divide block in half
- Transform right half
- Swap left and right halves
- Repeat some fixed number of times.

Security comes from complexity of the transformation.

Simplified DES

Simplified DES

- Simplified algorithm for teaching purposes

Simplified DES

- Simplified algorithm for teaching purposes
- Blocks: 12 bits

Simplified DES

- Simplified algorithm for teaching purposes
- Blocks: 12 bits
- Key: 9 bits

Simplified DES

- Simplified algorithm for teaching purposes
- Blocks: 12 bits
- Key: 9 bits
- Repeat for n rounds

Simplified DES

- Simplified algorithm for teaching purposes
- Blocks: 12 bits
- Key: 9 bits
- Repeat for n rounds

Not secure.

Simplified DES Algorithm

Simplified DES Algorithm

Key

9-bit key.

Simplified DES Algorithm

Key

9-bit key.

For ith round, use K_i: eight bits starting with ith bit.

Simplified DES Algorithm

Key

9-bit key.

For ith round, use K_i: eight bits starting with ith bit.

Algorithm

Divide 12-bit block into $L_0 R_0$

Simplified DES Algorithm

Key

9-bit key.

For ith round, use K_i: eight bits starting with ith bit.

Algorithm

Divide 12-bit block into $L_0 R_0$

For ith round:

- Compute $f(R_{i-1}, K_i)$

Simplified DES Algorithm

Key

9-bit key.

For ith round, use K_i: eight bits starting with ith bit.

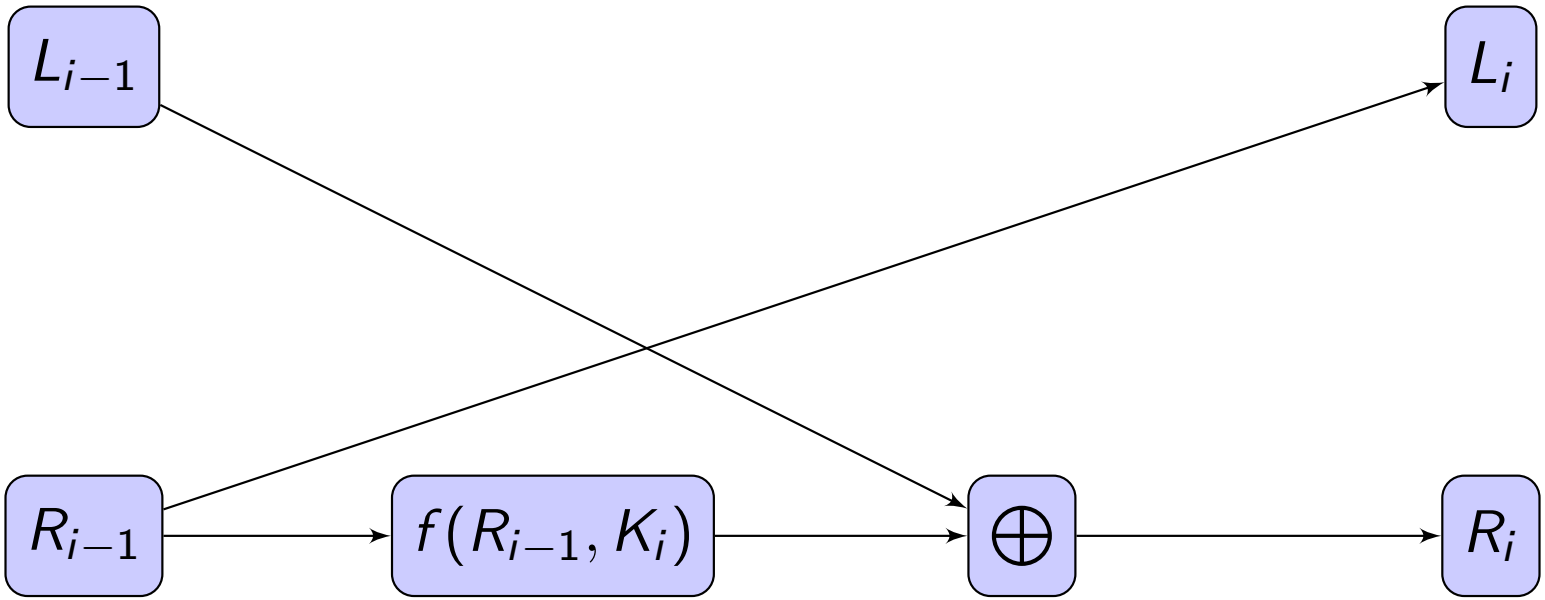
Algorithm

Divide 12-bit block into $L_0 R_0$

For ith round:

- Compute $f(R_{i-1}, K_i)$
- $L_i = R_{i-1}$
- $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$

Diagram of ith round



The function f

The function f

- Expand R_{i-1} to eight bits

The function f

- Expand R_{i-1} to eight bits
- Compute $E(R_{i-1}) \oplus K_i$

The function f

- Expand R_{i-1} to eight bits
- Compute $E(R_{i-1}) \oplus K_i$
- Split into two four-bit strings

The function f

- Expand R_{i-1} to eight bits
- Compute $E(R_{i-1}) \oplus K_i$
- Split into two four-bit strings
- Transform each four-bit string via S-box

The function f

- Expand R_{i-1} to eight bits
- Compute $E(R_{i-1}) \oplus K_i$
- Split into two four-bit strings
- Transform each four-bit string via S-box

The S-box

- Highly non-linear transformation

The function f

- Expand R_{i-1} to eight bits
- Compute $E(R_{i-1}) \oplus K_i$
- Split into two four-bit strings
- Transform each four-bit string via S-box

The S-box

- Highly non-linear transformation
- Comes from a lookup table

The function f

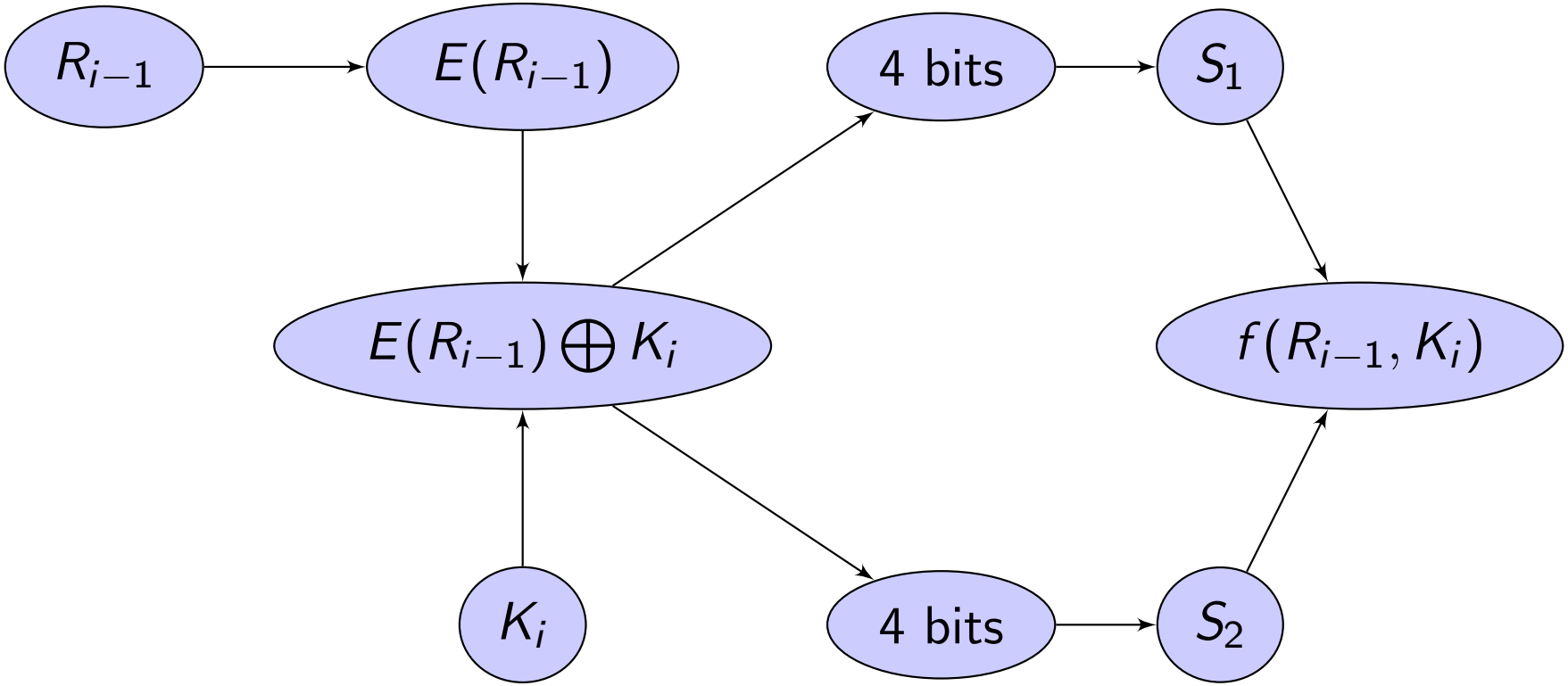
- Expand R_{i-1} to eight bits
- Compute $E(R_{i-1}) \oplus K_i$
- Split into two four-bit strings
- Transform each four-bit string via S-box

The S-box

- Highly non-linear transformation
- Comes from a lookup table

	000	001	010	011	100	101	110	111
0	101	010	001	110	011	100	111	000
1	011	100	110	010	000	111	101	011

Diagram of f



History of DES

History of DES

- Developed in 1970s at IBM

History of DES

- Developed in 1970s at IBM
- Modified by NSA to prevent differential cryptanalysis

History of DES

- Developed in 1970s at IBM
- Modified by NSA to prevent differential cryptanalysis
- Official standard in 1977

History of DES

- Developed in 1970s at IBM
- Modified by NSA to prevent differential cryptanalysis
- Official standard in 1977
- Thoroughly broken by 1999. Key broken in 22 hours and 15 minutes.

Structure of DES

Structure of DES

Properties

- 64-bit blocks;

Structure of DES

Properties

- 64-bit blocks; 56-bit key;

Structure of DES

Properties

- 64-bit blocks; 56-bit key; 16 rounds

Structure of DES

Properties

- 64-bit blocks; 56-bit key; 16 rounds
- "Feistel structure" combines permutations with S-boxes

Structure of DES

Properties

- 64-bit blocks; 56-bit key; 16 rounds
- "Feistel structure" combines permutations with S-boxes
- Efficient hardware implementation, but slow in software

Structure of DES

Properties

- 64-bit blocks; 56-bit key; 16 rounds
- "Feistel structure" combines permutations with S-boxes
- Efficient hardware implementation, but slow in software
- Vulnerable to brute force because of small key size

Structure of DES

Properties

- 64-bit blocks; 56-bit key; 16 rounds
- "Feistel structure" combines permutations with S-boxes
- Efficient hardware implementation, but slow in software
- Vulnerable to brute force because of small key size
- Linear cryptanalysis breaks in 2^{43} steps

Structure of DES

Properties

- 64-bit blocks; 56-bit key; 16 rounds
- "Feistel structure" combines permutations with S-boxes
- Efficient hardware implementation, but slow in software
- Vulnerable to brute force because of small key size
- Linear cryptanalysis breaks in 2^{43} steps — if you have 2^{43} known plaintexts!

Triple DES

Triple DES

Triple DES

Triple DES

Triple DES

- Encrypt with DES three times

Triple DES

Triple DES

- Encrypt with DES three times
- Either two or three keys

Triple DES

Triple DES

- Encrypt with DES three times
- Either two or three keys
- Secure but slow

Triple DES

Triple DES

- Encrypt with DES three times
- Either two or three keys
- Secure but slow
- Break in 2^{113} steps with 2^{32} known plaintexts

Advanced Encryption Standard

AES

Advanced Encryption Standard

AES

- Adopted in 2001 after NIST competition

Advanced Encryption Standard

AES

- Adopted in 2001 after NIST competition
- 128-bit blocks;

Advanced Encryption Standard

AES

- Adopted in 2001 after NIST competition
- 128-bit blocks; 128, 192, or 256 bit key;

Advanced Encryption Standard

AES

- Adopted in 2001 after NIST competition
- 128-bit blocks; 128, 192, or 256 bit key; 10, 12, or 14 rounds

Advanced Encryption Standard

AES

- Adopted in 2001 after NIST competition
- 128-bit blocks; 128, 192, or 256 bit key; 10, 12, or 14 rounds
- Matrix operations over a finite field $\mathbb{F}_{2^8}$

Advanced Encryption Standard

AES

- Adopted in 2001 after NIST competition
- 128-bit blocks; 128, 192, or 256 bit key; 10, 12, or 14 rounds
- Matrix operations over a finite field $\mathbb{F}_{2^8}$
- Best known attack: $2^{126.1}$, $2^{189.7}$, or $2^{254.4}$ steps.

The Best of Both Worlds

- Generate a symmetric cipher key

The Best of Both Worlds

- Generate a symmetric cipher key
- Use an asymmetric cipher to transmit the key

The Best of Both Worlds

- Generate a symmetric cipher key
- Use an asymmetric cipher to transmit the key
- Communicate using your fast symmetric cipher