
Block Ciphers, Hashes

16 March 2011

Lecture 4

Slide Credits: Steve Zdancewic (UPenn)

Topics for Today

- Shared Key Encryption
 - Triple-DES (3DES)
 - AES
- Block Cipher Modes
- Cryptographic Hashes

- Sources: HAC 7.2.2, 9.1-9.4, 12.6.1

Block Cipher Performance

Algorithm	Key Length	Block Size	Rounds	Clks/Byte
Twofish	variable	128	16	18.1
Blowfish	variable	64	16	19.8
Square	128	128	8	20.3
RC5-32/16	variable	64	32	24.8
CAST-128	128	64	16	29.5
DES	56	64	16	43
Serpent	128,192,256	128	32	45
SAFER (S)K-128	128	64	8	52
FEAL-32	64, 128	64	32	65
IDEA	128	64	8	74
Triple-DES	112	64	48	116

Triple-DES

- DES was attackable – but still only by brute force
 - Increase the key length!
 - How?
 - Many hardware implementations of DES existed and it had been basically proven secure
 - Why not just encrypt it twice and thereby increase the security?
-

Some options:

1. $E(k_1, E(k_1, \text{plaintext}))$
 - Doesn't increase the key space at all! Why?
1. $E(k_2, E(k_1, \text{plaintext}))$
 - Interestingly only **doubles** the key space (same as 2^{57} , not what we want)

Solution: $E(k_1, D(k_2, E(k_1, \text{plaintext})))$

- Encrypt with k_1 , decrypt with k_2 , encrypt with k_1
 - Increases the key space to 2^{112} , at the price of three times the operations (**Triple-DES**)
-

Advanced Encryption Standard (AES)

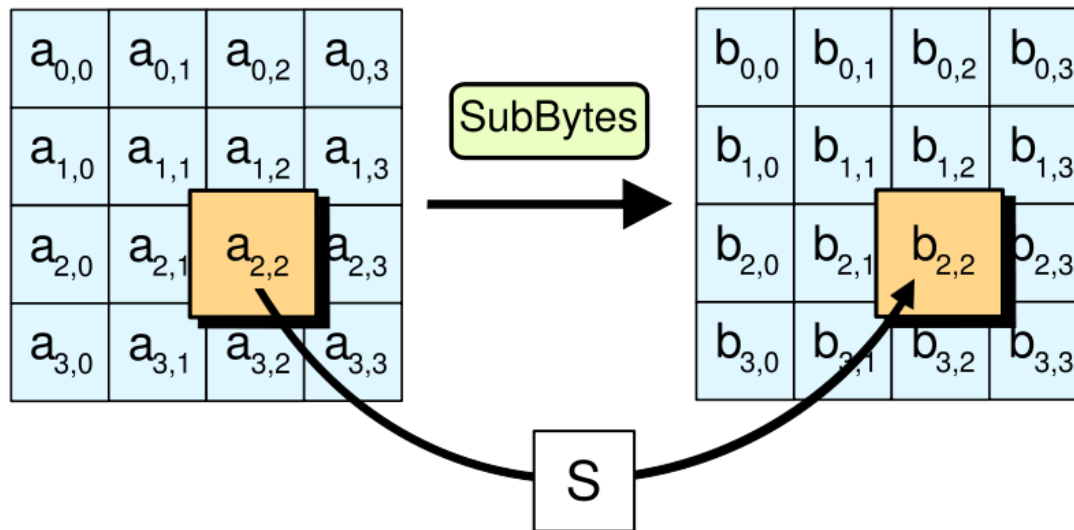
- National Institute of Standards & Technology NIST
 - Computer Security Research Center (CSRC)
 - <http://csrc.nist.gov/>
 - <http://www.esat.kuleuven.ac.be/~rijmen/rijndael/>
- Uses the Rijndael algorithm
 - Invented by Belgium researchers
Dr. Joan Daemen & Dr. Vincent Rijmen
 - Adopted May 26, 2002
 - Key length: 128, 192, or 256 bits
 - Block size: 128 (192, or 256) bits

Advanced Encryption Standard (AES)

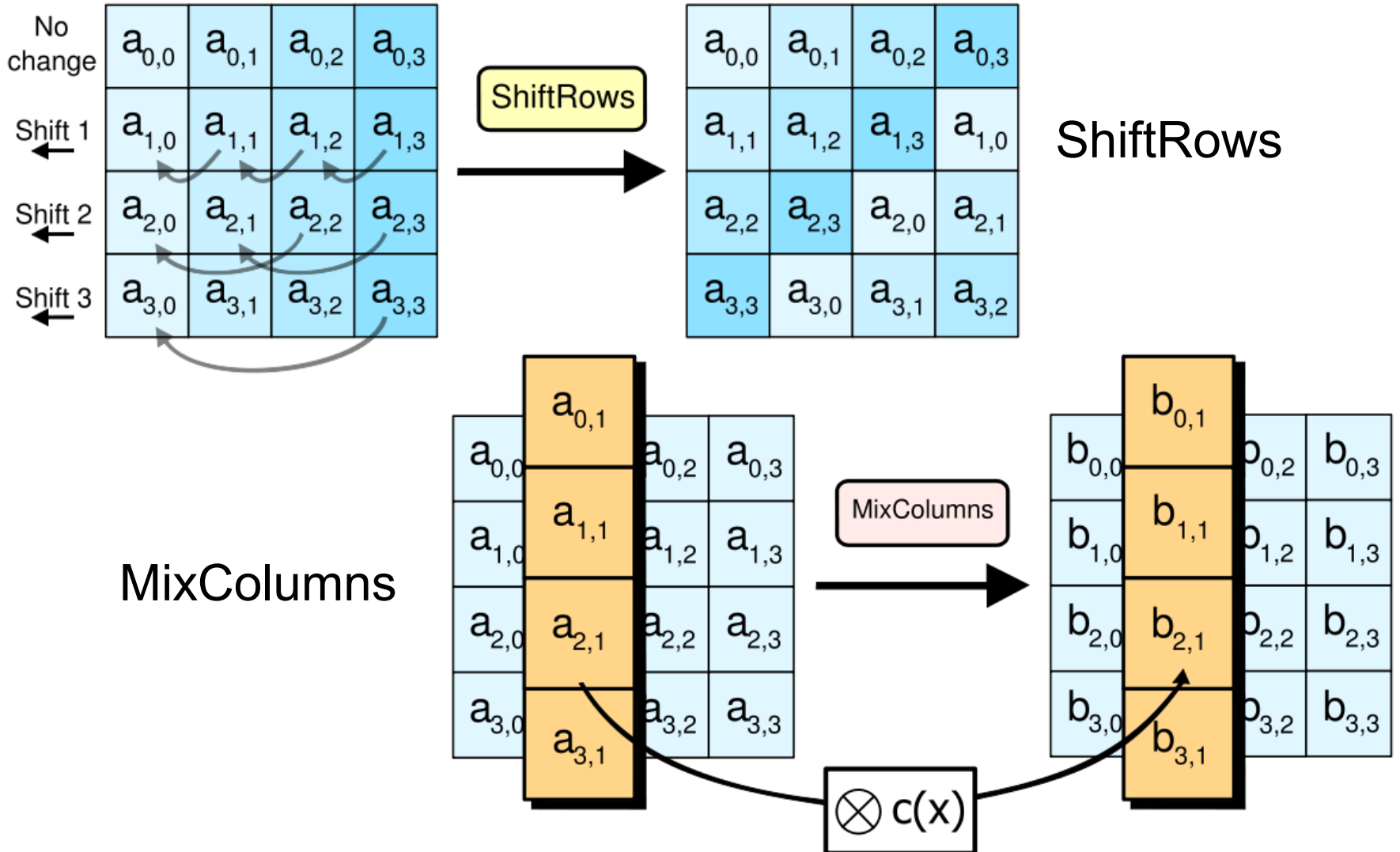
- Differs from DES in that
 - Variable number of rounds
 - Variable key size (128, 192 ,256)
 - Not Feistel - works on the whole message at once
 - Includes columnar transposition in addition to permutations
- AES operations
 - Substitution (SBoxes)
 - Row Shifts
 - Column Combinations
- Has held up to public scrutiny for now
 - Read more on it and how it works on Wikipedia

AES Operations

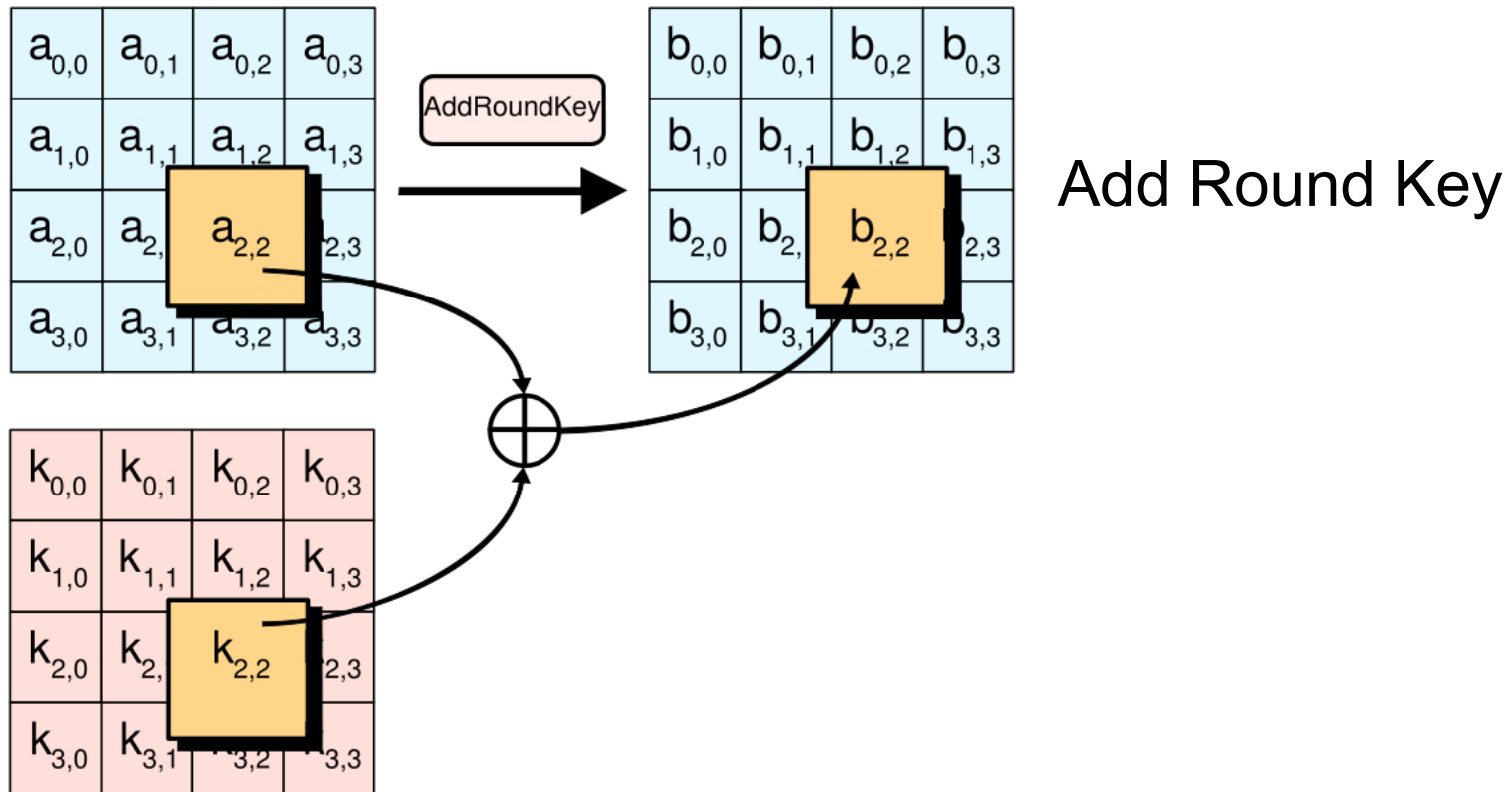
SubBytes Substitution



AES Operations



AES Operations



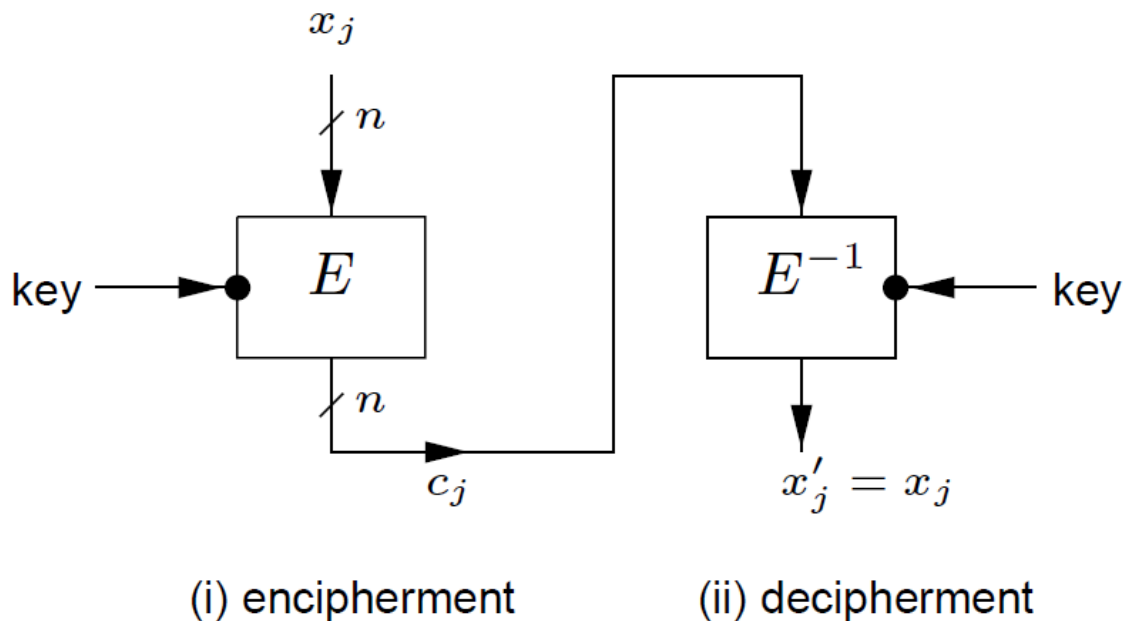
Block Cipher Modes

- What do we do with a block cipher of size n if the message size is greater than n ?

Electronic Code Book (ECB)

- Simplest idea: Break the message into n bit blocks and encipher each one independently

a) Electronic Codebook (ECB)



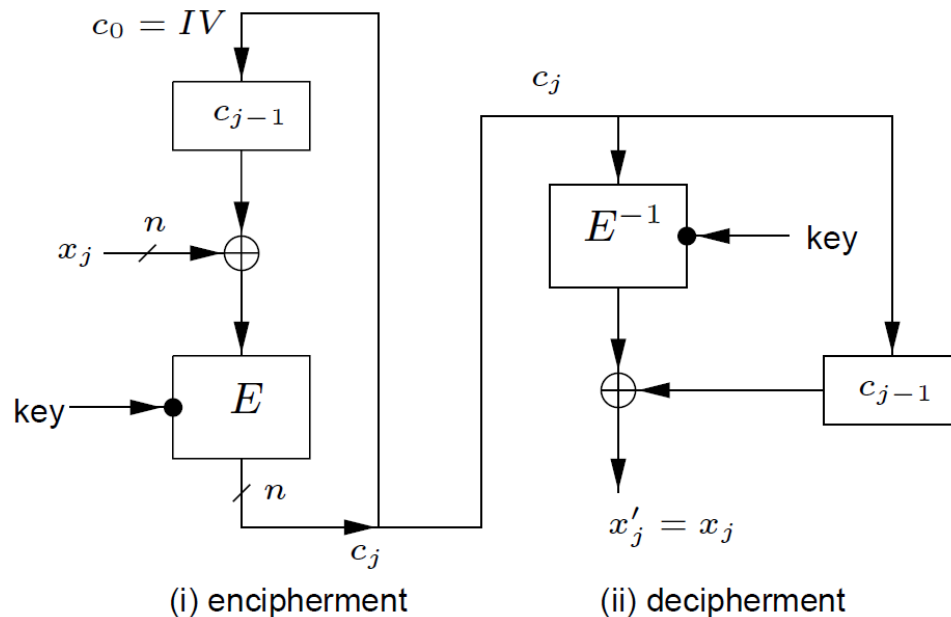
ECB Properties

- **Identical plaintext** blocks (under the same key) result in identical ciphertext
 - Preserves patterns in messages
- **No Chaining Dependencies:** blocks are enciphered independently of all other blocks. Re-ordering ciphertext blocks results in corresponding re-ordered plaintext blocks
- **Error propagation:** one or more bit errors in a single ciphertext block affect decipherment of that block only

Cipher Block Chaining (CBC)

- Chain each block based on the previous one
 - Introduce randomness to each block
 - Introduce dependencies in the message
- Use an Initialization Vector (IV) for the first block

b) Cipher-block Chaining (CBC)



CBC Properties

- **Identical plaintexts**: identical ciphertext blocks result when the same plaintext is enciphered under the same key and IV
- **Chaining dependencies**: the chaining mechanism causes ciphertext c_j to depend on x_j and all preceding plaintext blocks
 - The entire dependency on preceding blocks is, however, contained in the value of the previous ciphertext block.
- **Error propagation**: a single bit error in ciphertext block c_j affects decipherment of blocks c_j and c_{j+1} (since x_j depends on c_j and c_{j-1}).
 - Block x'_j recovered from c_j is typically totally random (50% in error)
 - The recovered plaintext x'_{j+1} has bit errors precisely where c_j did.
 - Thus an adversary may cause predictable bit changes in x_{j+1} by altering corresponding bits of c_j
- **Error recovery**: the CBC mode is *self-synchronizing* in the sense that if an error (including loss of one or more entire blocks) occurs in block c_j but not c_{j+1} , c_{j+2} is correctly decrypted to x_{j+2}

So Far

- Shared Key Encryption
 - AES
- Block Cipher Modes
- Cryptographic Hashes

Hash Algorithms

- Hash function defined by:
 - Compression
 - Take a variable length string, Produce a fixed length digest
 - Typically 128-1024 bits
 - Ease of Computation



- (Noncryptographic) Examples:
 - Parity (or byte-wise XOR)
 - CRC (cyclic redundancy check) used in communications
 - Ad hoc hashes used for hash tables
- Realistic Example
 - The NIST Secure Hash Algorithm (SHA) takes a message of less than 2^{64} bits and produces a digest of 160 bits

Cryptographic Hashes

- Create a hard-to-invert summary of input data
- Useful for integrity properties
 - Sender computes the hash of the data, transmits data and hash
 - Receiver uses the same hash algorithm, checks the result
- Like a check-sum or error detection code
 - Uses a cryptographic algorithm internally
 - More expensive to compute
- Sometimes called a Message Digest
- History:
 - Message Digest (MD4 -- invented by Rivest, MD5)
 - Secure Hash Algorithm - 1993 - (SHA-0)
 - Secure Hash Algorithm (SHA-1)
 - SHA-2 (actually a family of hash algorithms with varying output sizes)
- Attacks have been found against both SHA-0 and SHA-1

Uses of Hash Algorithms

- Hashes are used to protect *integrity* of data
 - Virus Scanners
 - Program fingerprinting in general
 - Modification Detection Codes (MDC)
- Message Authenticity Code (MAC)
 - Includes a cryptographic component
 - Send (msg, hash(msg, key))
 - Attacker who doesn't know the key can't modify msg (or the hash)
 - Receiver who knows key can verify origin of message
- Make digital signatures more efficient (we'll see this later)

Conclusion

- Shared Key Encryption
 - AES
- Block Cipher Modes
- Cryptographic Hashes

- Enjoy your break