CMSC 426
Principles of Computer Security

Introduction to Cryptology

Last Class We Covered

- Exam!!!

- Hope to get them graded before next class
  - (No promises, though!)

Any Questions from Last Time?

Today's Topics

- Introduction to crypto
  - Ciphers
- Block ciphers
  - DES
  - 3DES
  - AES

Crypto Definitions

Crypto-

- Cryptography
  - “Hidden writing”
  - Creation and use of secret codes and data-related security measures
- Cryptanalysis
  - Theory and practice of “breaking” cryptographic protocols
  - “Breaking” means recovering protected text/bypassing security
- Cryptology
  - The study of coded messages
  - Scientific study of codes: creating, using, analyzing, “breaking”

Encryption Types

- Encryption
  - Turning plain text into encrypted, “protected” text
- Decryption
  - Returning encrypted text to a readable, plain text state

- Symmetric Encryption
  - Uses the same key for encryption and decryption
- Asymmetric Encryption
  - Uses different keys for encryption and decryption

Symmetric Encryption

Components of Symmetric Encryption

- Plaintext
- Ciphertext
- Encryption algorithm
- Secret key
- Decryption algorithm

- Example: Vigenère cipher
  - “ATTACK AT DAWN” with “DOG” as the keyword
  - Ciphertext is “DHZDQQ DH JDKT”

Historical Ciphers (Algorithms)

- Caesar cipher
  - "Rotation" of the alphabet
- Atbash cipher
  - "Reversal" of the alphabet
- Keyword cipher
  - Keyword "begins" the alphabet, rest follows in order
  - "Cryptography": CRYPTOGAHBDEFIJKLMNQSUVWXZ
- Vigenère cipher
  - Keyword is repeated, and is used to shift plaintext into ciphertext

Substitution Cipher Example

- Assume an “alphabet” of 38 characters: A-Z, 0-9, “ ”, and .

- The substitution cipher is random in this case – there is no keyword or simple reversal/shift of the alphabet
  - **`PX2LOB.1MWGSU0V5H6TYNF9K IA7QO3ZJRE4CD8`**

- What is the plaintext, ciphertext, encryption algorithm, secret key, and decryption algorithm in this case?

Substitution Cipher Example

- Plaintext
- Ciphertext
  - Both are a message written in the 38-character alphabet
- Encryption algorithm
  - Application of the substitution cipher to the original message
- Secret Key
  - The substitution ciphered alphabet
- Decryption algorithm
  - Application of the inverse of the substitution cipher

Block Ciphers
(Symmetric Block Encryption)

Block Ciphers

- Process the plaintext in fixed-size “blocks” (hence the name)
- Ciphertext produced is of blocks of equal size

- Block ciphers are symmetric algorithms
  - Key remains the same for encryption and decryption
  - However, two separate algorithms for en/decryption

- Most commonly-used algorithms are DES, 3DES, and AES

Block Cipher Algorithms

- Sequence of rounds, made of permutations and substitutions
  - Each round has its own unique subkey value, derived from the key
- DES and 3DES both use a Feistel network structure
  - Basic encryption and decryption algorithm are the same
    - Only difference is the order in which subkeys are applied
  - 16 rounds of en/decryption
  - Makes use of XOR and substitution

Components of Block Ciphers

- Block size
  - Size in bits of a plaintext/ciphertext block (commonly 128 bits)
- Key size
  - Size in bits of the key (commonly 128 bits)
- Round function
  - Basic encryption function; iterated to form the encryption algorithm
- Number of rounds
  - The number of iterations of the round function
- Subkey algorithm
  - Algorithm that expands the key into multiple round keys

Feistel Networks

- Iterative structure used in the DES and 3DES algorithms
  - Split 64 bits of input into right and left blocks
  - Apply Feistel function to the right half of the data
  - XOR it using the left half of the data
  - Swap the two blocks for the next round

  - Each of the 16 rounds is identical
    - *(Which is why we swap the data's sides)*
    - Only difference is the subkey used in the Feistel function

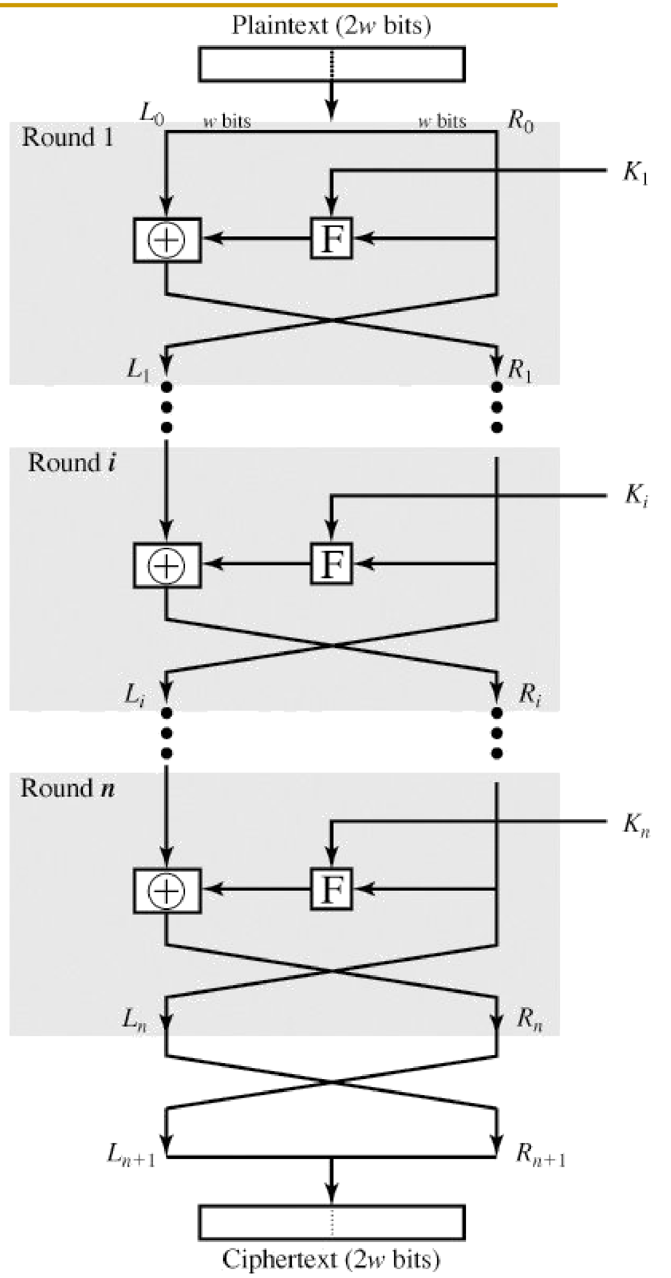
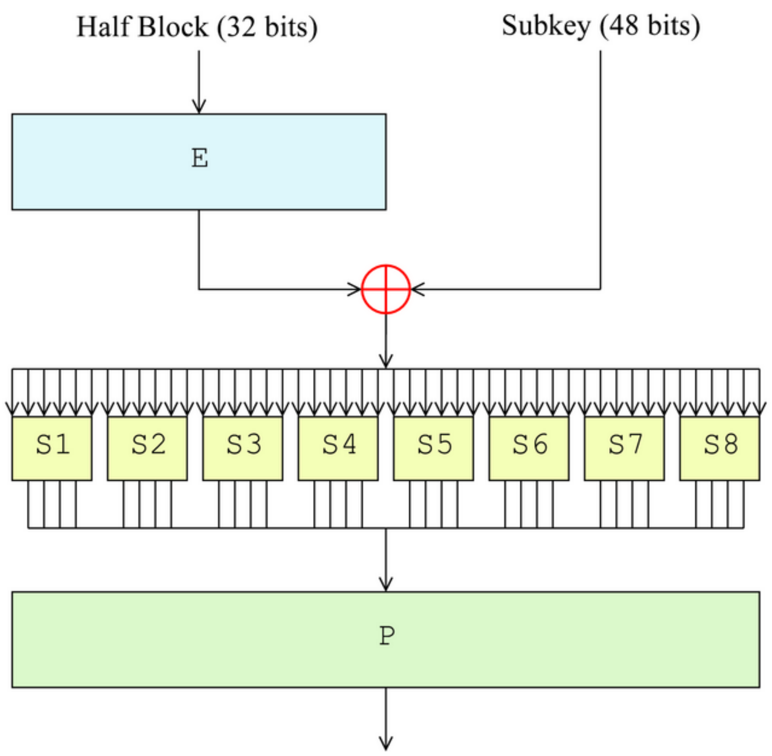


Image taken from Computer Security (Stallings & Brown)

Feistel Function



- Consists of four stages, done on 32 bits of data
- Expansion: 32 bits is expanded to 48 bits (eight 6 bit pieces, which each contain a copy of the adjacent bit on each side)
- Key mixing: XOR'd with 48-bit subkey
- Substitution: divided into eight 6 bit pieces again, which are processed by the substitution boxes (S-box)
  - Turns 6 bits in 4 bits according to a non-linear transformation (provided by a lookup table)
  - **Core component of the security of DES; without these, it would be trivial to break**
- Permutation: outputs are rearranged according to a fixed permutation, so that the same bits don't go through the same substitution box again together

Image and information taken from https://en.wikipedia.org/wiki/Data_Encryption_Standard

DES (Data Encryption Standard)

- Blocks are 64 bits
- Key is 56 bits
  - Actually 64 bits, but every 8th bit is a parity bit
- Algorithm itself is very secure
  - Very well-studied, and no reported fatal weaknesses
- Key size is woefully small
  - Only 72,000,000,000,000,000 possible keys
  - Can be brute-forced by a powerful machine in about an hour
- Adopted in 1977, but not used widely since the 90s

Triple DES (or 3DES)

- Uses 3 keys, for a total key size of 168 bits
  - Either two or three independent keys, depending on implementation

- To encrypt, it applies the original DES algorithm as follows:
  - Encrypt with key 1
  - Decrypt with key 2
  - Encrypt with key 3
  - (If only two keys used, duplicate is used as key 1 and key 3)

- Three times as slow as DES… not good for large encryption jobs

AES (Advanced Encryption Standard)

Advanced Encryption Standard

- AES is also a block cipher, but does not use Feistel networks
  - Instead of splitting data in half and using one half to modify the other, AES processes the entire data block in parallel

- Block length is 128 bits, and key can be 128, 192, or 256 bits
  - For purposes of this class, we'll assume the key is always 128 bits
    - With 128 bits, this means that AES performs 10 rounds

- Decryption is still performed with keys applied in reverse
  - But encryption and decryption algorithms are not identical as in DES

AES Algorithm Overview

- 128 bits of input are represented as a 4 by 4 array of bytes

$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$

- Four different stages are performed in each round
  - Substitute Bytes
  - Shift Rows
  - Mix Columns
  - Add Round Key

substitution steps

Skipped in last round.

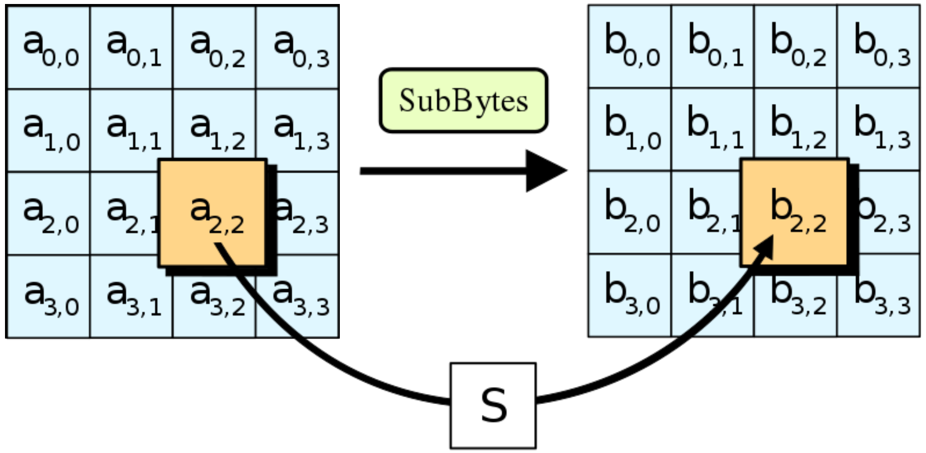
permutation step

Also occurs before the rounds begin.

Image and information taken from https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Substitute Bytes

- Uses an S-box to perform a table lookup that allows for a byte-by-byte substitution of the block



- Provides the non-linearity in the cipher
  - S-box is derived based on information from the key, using complex math we won’t cover in this class
    - (Multiplicative inverse, affine transformation, etc.)
  - When <u>de</u>crypting, this is the step that differs, creating a different, “inverse” S-box

Image and information taken from https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Shift Rows

- Each row is shifted by an offset
  - This means that each column now contains information from each row
- This prevents the columns in the 4 by 4 array from being encrypted together throughout all the rounds

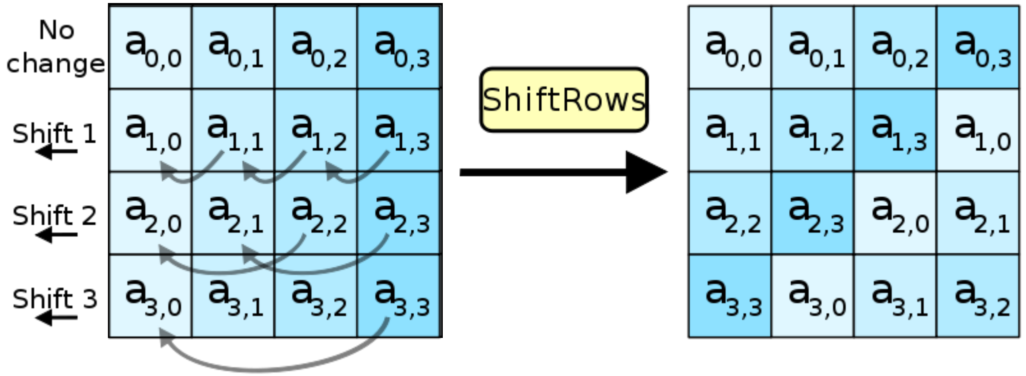
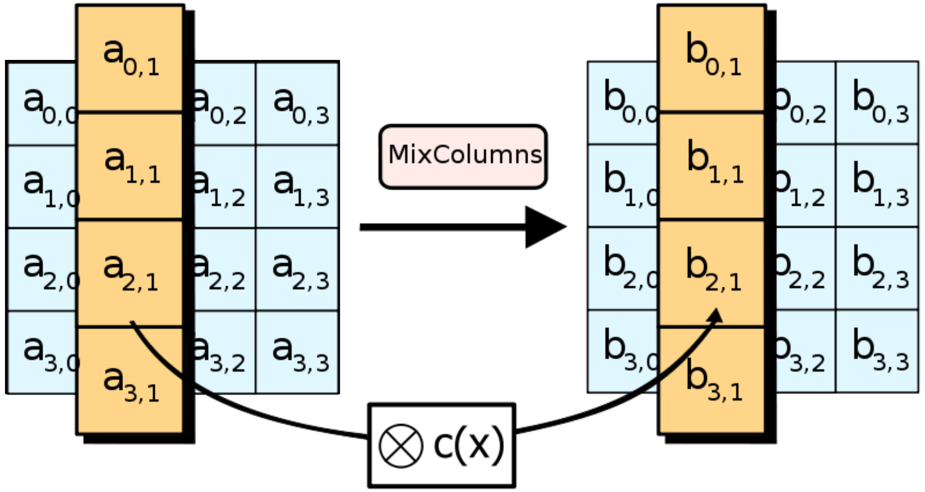


Image and information taken from https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Mix Columns

- Each column is altered, taking in the four bytes of the column, and outputting four bytes
- Each input byte affects all four output bytes (more math)
- This step does not occur in the final round of the algorithm



$$\begin{bmatrix} b_{0,j} \\ b_{1,j} \\ b_{2,j} \\ b_{3,j} \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} a_{0,j} \\ a_{1,j} \\ a_{2,j} \\ a_{3,j} \end{bmatrix} \qquad 0 \le j \le 3$$

Image and information taken from https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Add Round Key

- Before the rounds begin, the original 128 bit key is expanded into an array of subkeys for each round
- Simple bitwise XOR of the current block with that round's subkey
- This stage also occurs initially, before the rounds have properly begun

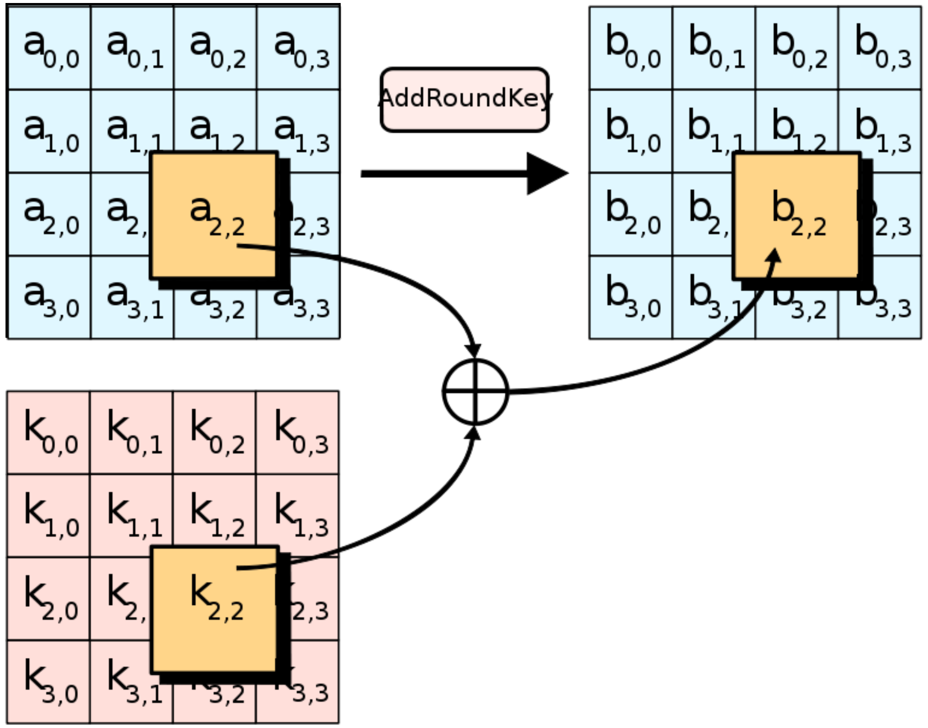


Image and information taken from https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Announcements

- Paper 2&3 and Homework 2 will be released later today
  - Homework 2 will be due next Wednesday (17th)
  - Paper 2&3 will be due October 24th

- Lab 2 is due next Wednesday (17th)