Course Business

- Midterm is on March 1
  - Allowed to bring one index card (double sided)
- Final Exam is Monday, May 1 (7 PM)
  - Location: Right here

Cryptography
CS 555

Topic 18: AES, Differential Cryptanalysis, Hashing

Recap

Goals for This Week:

- Practical Constructions of Symmetric Key Primitives

Last Class: DES/3DES

- 16 round Feistel Network
- DES can now be broken by brute-force attacks in practice

Today's Goals: AES/Hash Functions

Advanced Encryption Standard (AES)

- (1997) US National Institute of Standards and Technology (NIST) announces competition for new block cipher to replace DES
- Fifteen algorithms were submitted from all over the world
  - Analyzed by NIST
- Contestants given a chance to break competitors schemes
- October, 2000 NIST announces a winner Rijndael
  - Vincent Rijmen and Joan Daemen
  - No serious vulnerabilities found in four other finalists
  - Rijndael was selected for efficiency, hardware performance, flexibility etc…

Advanced Encryption Standard

- **Block Size:** 128 bits (viewed as 4x4 byte array)
- **Key Size:** 128, 192 or 256

- Essentially a Substitution Permutation Network
  - **AddRoundKey:** Generate 128-bit sub-key from master key XOR with current state
  - **SubBytes:** Each byte of state array (16 bytes) is replaced by another byte according a a single S-box (lookup table)
  - **ShiftRows –** shift ith row by i bytes
  - **MixColumns –** permute the bits in each column

Substitution Permutation Networks

- S-box a public "substitution function" (e.g. $S \in \textbf{Perm}_8$).

- S is not part of a secret key, but can be used with one

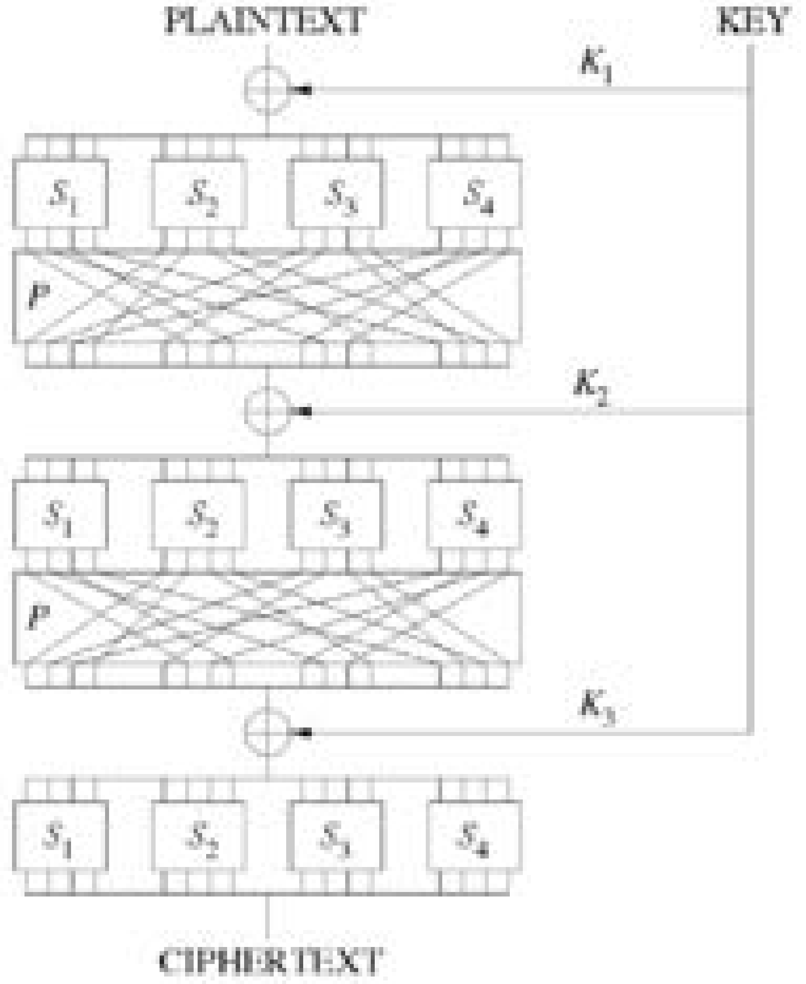
$$f(x) = S(x \oplus k)$$

Note: there are only n! possible bit mixing permutations of [n] as opposed to 2^n! Permutations of $\{0,1\}^n$

Input to round: x, k (k is subkey for current round)

1. **Key Mixing**: Set $x := x \oplus k$
2. **Substitution**: $x := S_1(x_1) \parallel S_2(x_2) \parallel \cdots \parallel S_8(x_8)$
3. **Bit Mixing Permutation**: permute the bits of x to obtain the round output

Substitution Permutation Networks



- **Proposition 6.3:** Let F be a keyed function defined by a Substitution Permutation Network. Then for any keys/number of rounds F_k is a permutation.

- Why? Composing permutations f,g results in another permutation h(x)=g(f(x)).

Advanced Encryption Standard

- Block Size: 128 bits
- Key Size: 128, 192 or 256

- Essentially a Substitution Permutation Network
  - **AddRoundKey:** Generate 128-bit sub-key from master key, XOR with current state array
  - **SubBytes:** Each byte of state array (16 bytes) is replaced by another byte according a single S-box (lookup table)
  - **ShiftRows**
  - **MixColumns**

Key Mixing

Permutation

Substitution

AddRoundKey:

Round Key (16 Bytes)

00001111			
10100011	…		
11001100		…	
01111111			…

$\oplus$

State

11110000			
01100010	…		
00110000		…	
11111111			…

$=$

11111111			
11000001	…		
11111100		…	
10000000			…

AddRoundKey:

Round Key (16 Bytes)

10100011	…		
		…	
			…

State

11111111			
11000001	…		
11111100		…	
10000000			…

SubBytes (Apply S-box)

S(11111111)			
S(11000001)	S(…)		
S(11111100)		S(…)	
S(10000000)			S(…)

AddRoundKey:

Round Key (16 Bytes)

10100011	…		
		…	
			…

State

S(11111111)			
S(11000001)	S(…)		
S(11111100)		S(…)	
S(10000000)			S(…)

Shift Rows

S(11111111)			
	S(11000001)	S(…)	
S(…)		**S(11111100)**	
		S(…)	**S(10000000)**

AddRoundKey:

Round Key (16 Bytes)

10100011	…		
		…	
			…

State

S(11111111)			
	S(11000001)	S(…)	
S(…)		**S(11111100)**	
		S(…)	**S(10000000)**

Mix Columns

Invertible (linear) transformation.

Key property: if inputs differ in b>0 bytes then output differs in 5-b bytes (minimum)

AES

- We just described one round of the SPN

- AES uses
  - 10 rounds (with 128 bit key)
  - 12 rounds (with 192 bit key)
  - 14 rounds (with 256 bit key)

AES Attacks?

- Side channel attacks affect a few specific implementations
  - But, this is not a weakness of AES itself
  - Timing attack on OpenSSL's implementation AES encryption (2005, Bernstein)

- (2009) Attack on 11 round version of AES
  - recovers 256-bit key in time 2^{70}
  - But AES is 14 round (with 256 bit key) so the attack doesn't apply in practice
- (2009) Attack on 192-bit and 256 bit version of AES
  - recovers 256-bit key in time $2^{99.5}$.

- First public cipher approved by NSA for Top Secret information

Differential Cryptanalysis

Basic Goal:

Find specific differences in the input that lead to specific differences in output with probability (slightly) greater than we would expect for a random permutation

- Suppose that we pick x_1 and x_2 uniformly at random subject to the constraint

$$x_1 \oplus x_2 = \Delta_x$$

- **Question**: What is the probability that?

$$F_k(x_1) \oplus F_k(x_2) = \Delta_y$$

Differential Cryptanalysis

- Suppose that we pick x_1 and x_2 uniformly at random subject to the constraint

$$x_1 \oplus x_2 = \Delta_x$$

- **Question**: What is the probability that?

$$F_k(x_1) \oplus F_k(x_2) = \Delta_y$$

- **Answer for Ideal Cipher:** $\approx 2^{-n}$

- **Possible Answer for Weak Block Cipher:** $p \gg 2^{-n}$

- Attacker who finds Δ_x and Δ_y such that $p \gg 2^{-n}$ can exploit this observation

Differential Cryptanalysis

- Start by finding differential(s) for S-Box
- How?
- Brute force!
- Use differential for S-box to construct differential for entire cipher

Differential Cryptanalysis

- **Question**: What is the probability that?

$$F_k(x_1) \oplus F_k(x_2) = \Delta_y$$

- **Answer for Ideal Cipher:** 2^{-n}

- **Example 1:** FEAL-8.
  - Differential cryptanalysis can quickly recover key after just 1,000 chosen plaintexts

- **Example 2:** DES.
  - Differential cryptanalysis can quickly recover key after ``just” 2^{43} known plaintext/ciphertext pairs
  - Differential Cryptanalysis discovered (publicly) after DES
  - NSA knew about differential cryptanalysis before DES

Hash Function from Block Ciphers

Davies-Meyer Construction

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

How to prove collision resistance?

- We don't actually know how if we only use the assumption that F is strong pseudorandom permutation
- We can prove collision resistance in the ideal-cipher model
  - All parties have oracle access to truly random keyed permutation F, F^{-1}

Hash Function from Block Ciphers

Davies-Meyer Construction

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

Theorem: If F is modeled as an ideal cipher then an attacker making $q < 2^{n/2}$ queries to F finds a collision with probability at most $\frac{q^2}{2^n}$.

Davies-Meyer Construction

- Security proof in ideal-cipher model may not translate to real world

- **Example**: Davies-Meyer + DES is broken.

Other Hashing Algorithms

- MD5
  - Chinese cryptanalysists found a collision in 2004
  - Collisions can now be found on a desktop PC in < 60 seconds
  - Extension of attacks generates “controlled collisions”
- SHA1, SHA2
  - Use Davies-Meyer Construction with special block ciphers
  - Theoretical analysis: can find SHA1 collision in time 2^{80}.
  - SHA2 is widely deployed (e.g., in Bitcoin, PBKDF2-SHA256)

SHA3 (Keccak)

- NIST announced public competition in 2007 for SHA3
  - In response to weaknesses of SHA1 and MD5
- (2012) NIST selected Keccak as the winner of the competition
  - Based on an (unkeyed) permutation with large block length
  - Uses sponge construction instead of Merkle-Damgard to handle arbitrary length inputs
  - Very different from SHA1 and SHA2
- Proof of security in random-permutation model
  - Weaker than ideal-cipher model

Next Class

- Read Katz and Lindell 7.1-7.2, 7.5
- Theoretical Foundations for Symmetric Key Cryptography
  - One Way Functions
  - Pseudo randomness