Asymmetric-key Encryption

Dawn Song
dawnsong@cs.berkeley.edu

Review

- Introduction to cryptography
- Symmetric-key encryption
- One-time pad
- Block cipher
  - DES
    - Fiestel Networks
  - AES

Today

- Stream ciphers
- Modes of operation for Block ciphers
- Administrative matters
- Modular Arithmetic
- 5-min break
- Asymmetric-key encryption

Stream Cipher

- Pseudo-random generator
  - $F(k,i) = r_i$
  - k is secret
  - Attacker cannot distinguish $r_1, r_2, \ldots r_i$, from a sequence of random numbers
- Encrypt using stream ciphers
  - Alice and Bob share k
  - Alice wishes to send n-bit msg M = M1…Mn
  - $Ci = Mi \oplus F(k,i)$
  - Practical “one-time pad”

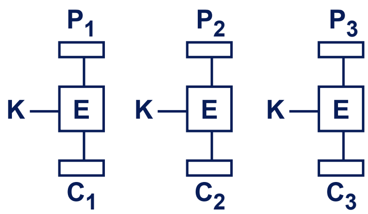
Block-cipher Modes of Operation

- Block-cipher has fixed block size
- How to encrypt arbitrary length msgs using a block cipher?
- How to ensure the same plaintext when encrypted/sent twice, will result in different ciphertexts?
- Different block-cipher modes of operation
  - Encryption scheme
    - Randomized, i.e., flips a coin
    - Stateful, i.e., depending upon state info
  - Decryption scheme
    - Neither randomized nor stateful
    - Why?

Examples of Block-Cipher Modes of Operation

- ECB: Electronic code book
- CBC: Cipher block chaining
- OFB: Output feedback
- CTR: Counter mode

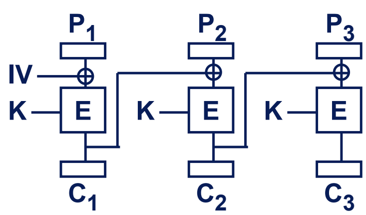
Electronic Code Book (ECB) Mode



- **Disadvantages and issues to note**
  - Same plaintext always corresponds to same ciphertext
  - Traffic analysis yields which ciphertext blocks are equal → know which plaintext blocks are equal
  - Adversary can replace blocks with other blocks

Cipher Block Chaining (CBC) Mode

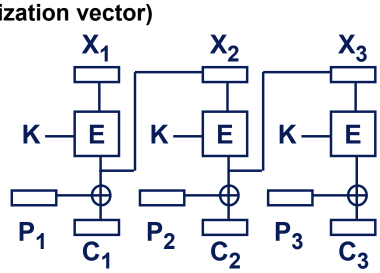
- $C_j = \{ P_j \oplus C_{j-1} \}_K$
- C_0 = IV (initialization vector)



- **Issues to note**
  - Altered ciphertext only influences two blocks

Output Feedback (OFB) Mode

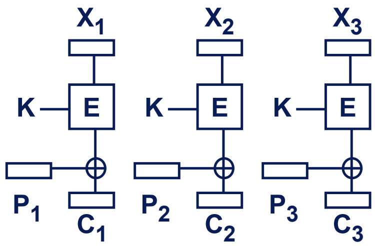
- X_1 = IV (initialization vector)
- $X_j = \{ X_{j-1} \}_K$
- $C_j = X_{j+1} \oplus P_j$



- **Issues to note**
  - Altered ciphertext only influences single block

Counter Mode (CTR)

- X_1 = IV called initialization vector
- $X_j = X_1 + j - 1$
- $C_j = \{ X_j \}_K \oplus P_j$



- Advantages
  - Easy to parallelize
- Issues to note
  - Altered ciphertext only influences single block

Administrative Matters (I)

- New TA: Rusty Sears
- Office hours on-line
  - M-W, F
- HW1 out
- Computer accounts and facility support

Administrative Matters (II)

- In order to turn in HW1's programming assignment, you will need a named UNIX account.
- If you do not already have one, you can set it up in 273 Soda (or any other instructional computer lab)
- Log into a machine with the username "newacct" and password "newacct"
- You will need to provide your student ID
- It takes approximately one business day for new account requests to be processed
- Contact TAs if you have problems

Modular Arithmetic

- a + b mod s
  - O($\log^2$ s)
- a*b mod s
  - O($\log^2$ s)
- a^b mod s
  - how to compute a^{25} mod s ?
  - Repeated squaring
    - » $a^{16} * a^8 * a^1$ mod s
  - O(($\log^2$ s) (log b))

Modular Division

- How to compute 1/a mod s?
- What does it mean?
  - $ax \equiv 1$ mod s
- Can it always be computed?
  - iff gcd (a,s) = 1
- How?
  - Extended Euclidean algorithm

Euclidean Algorithm

- Compute gcd (a,b)
- Lemma If a > b, then gcd(a,b) = gcd (a mod b, b)
  - Why?
- Euclid algorithm:
  - $b \leq a$,
  - Euclid (a,b) = Euclid (b, a mod b) if $b \neq 0$
    or a if b = 0

Extended Euclidean Algorithm

- For any positive integers a, b, the extended Euclidean algorithm returns integers x, y such that ax + by = gcd (a,b)
- How to use it to compute x such that $ax \equiv 1 \bmod s$?
- gcd (a,s) = 1, thus can compute x, y s.t. ax + sy = 1
  - Thus, $ax \equiv 1 \bmod s$
- If u is relatively prime to s>u, then u has a multiplicative inverse modulo s, which can be found in $O(\log^3 s)$

Asymmetric-key Crypto

- Symmetric cryptography: both parties share the same key
  - Secret key (or shared key) only known to communicating parties
- Asymmetric cryptography: each party has a public and a private key
  - Public key known to everyone
  - Private key only known to owner
- Requirements for secure communication
  - Symmetric crypto: key is secret and authentic
  - Asymmetric crypto: private key is secret and public key is authentic

Advantage of Public-Key Crypto

- Consider N parties, how can any pair of them establish a secret key?
  - To use symmetric-key crypto, requires secret and authentic channel to set up shared secret key
  - Need $O(N^2)$ keys
  - Key management is challenging
- Public-key crypto advantage
  - Each party only needs to know N-1 authentic public keys

Asymmetric-key Encryption

- encryption-Key ≠ decryption-Key
- Alice has public key: pub_key, private key: priv_key
- Bob wants to send Alice message M
- C = E(pub_key, M);
- M = D(priv_key, C)

Asymmetric cryptography

- encryption-Key ≠ decryption-Key
- We cannot simply run operations backwards
- Some things are hard to reverse
  - Often "hard" means "not in P"
  - Cryptanalysis is always easy in NP
  - Does P = NP?
- Multiplication
  - Easy to multiply two large primes
  - Hard to factor
  - Factoring up to 663 bits (200 digits) now demonstrated
    - » Intensive computing; record set in May 2005
  - More efficient factoring methods unknown

Using hard problems to make crypto

- Gauss (building on work by Fermat) proved
  - If p and q are primes and
  - If m is not a multiple of p or q
  - Then $m^{(p-1)(q-1)} = 1 \bmod pq$
- Example, p=3, q=5, pq = 15, (p-1)(q-1) = 8
  - $1^8 = 1 = 1 \bmod 15$
  - $2^8 = 256 = 1 \bmod 15$
  - $4^8 = 65536 = 1 \bmod 15$
  - $7^8 = 5764801 = 1 \bmod 15$
  - $8^8 = 16777216 = 1 \bmod 15$
  - $11^8 = 214358881 = 1 \bmod 15$
  - $13^8 = 815730721 = 1 \bmod 15$
  - $14^8 = 1475789056 = 1 \bmod 15$