

Exam 1 Review

CS461/ECE422 Fall 2007

Exam guidelines

- A single page of supplementary notes is allowed
- Closed book
- A calculator is allowed. (and strongly suggested for this exam)
- Students should show work on the exam. They can use supplementary sheets of paper if they run out of room.
- Students can use scratch paper if desired.

Exam logistics

- Exam will be given in the evening (7-8:15pm) in 112 and 114 of the Transportation Building
 - <http://webtools.uiuc.edu/ricker/CampusMap?target=s>
- Students will be split by last name

Topics

- Introductory definitions
- Risk Analysis
- Historical Cryptography
- Symmetric Cryptography
- Public or Asymmetric Cryptography
- Key Management
- Security Policies

Risk Analysis

- Understand
 - Assets
 - Vulnerabilities
 - Threats
 - Risk
- Qualitative vs Quantitative Analysis
 - Quantitative identifies absolute numbers for risk probability and asset value, so can calculate risk exposure, risk leverage

Security Policy

- Defines what needs to be done, not how
 - How is mechanism or control
- Organizational or natural language policies
- Formal policy languages
 - Control mechanism operation
 - In theory policy language could be applied to multiple types of mechanisms

Historical Ciphers

- Transposition
 - N-columnar transposition
- Substitution
 - Caesar, vigenere, book, one-time pad, enigma
- Language-based statistical attacks

Symmetric Encryption

- Block vs stream encryption
 - $P = b_0, b_1, \dots, b_n$
 - $E(P, k) = E(b_0, k_0) \parallel E(b_1, k_1) \parallel \dots$
 - If all k_i 's are equal and $\text{sizeof}(b_i)$ generally > 1 , $E(P, k)$ is a block cipher
- DES
 - Feistel network
 - Combination of p-boxes and s-boxes
 - 56 bit key and 64 bit block

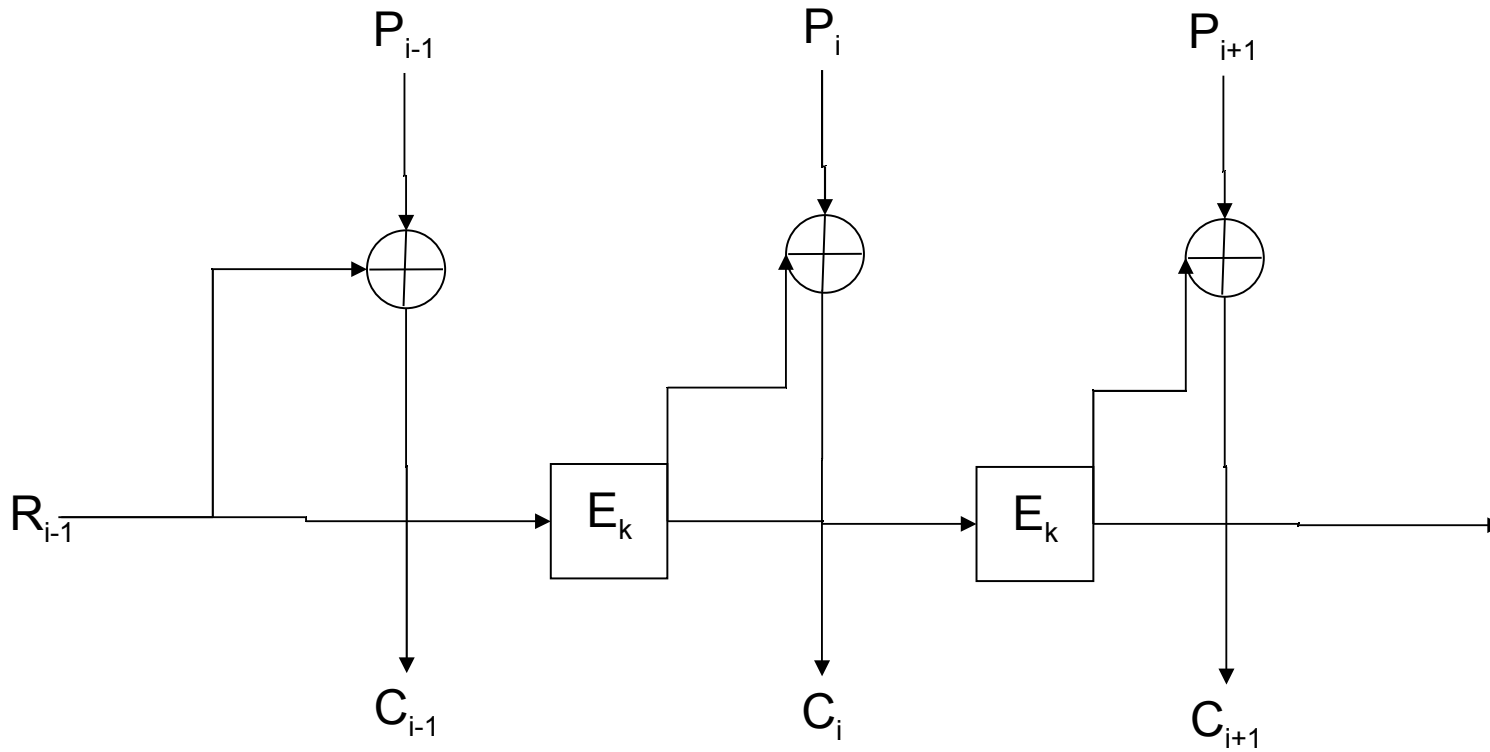
Symmetric Encryption

- AES
 - Iterative encryption
 - Multiple key sizes: 128, 192, 256
 - Block size: 128
 - 1 S box and various permutations

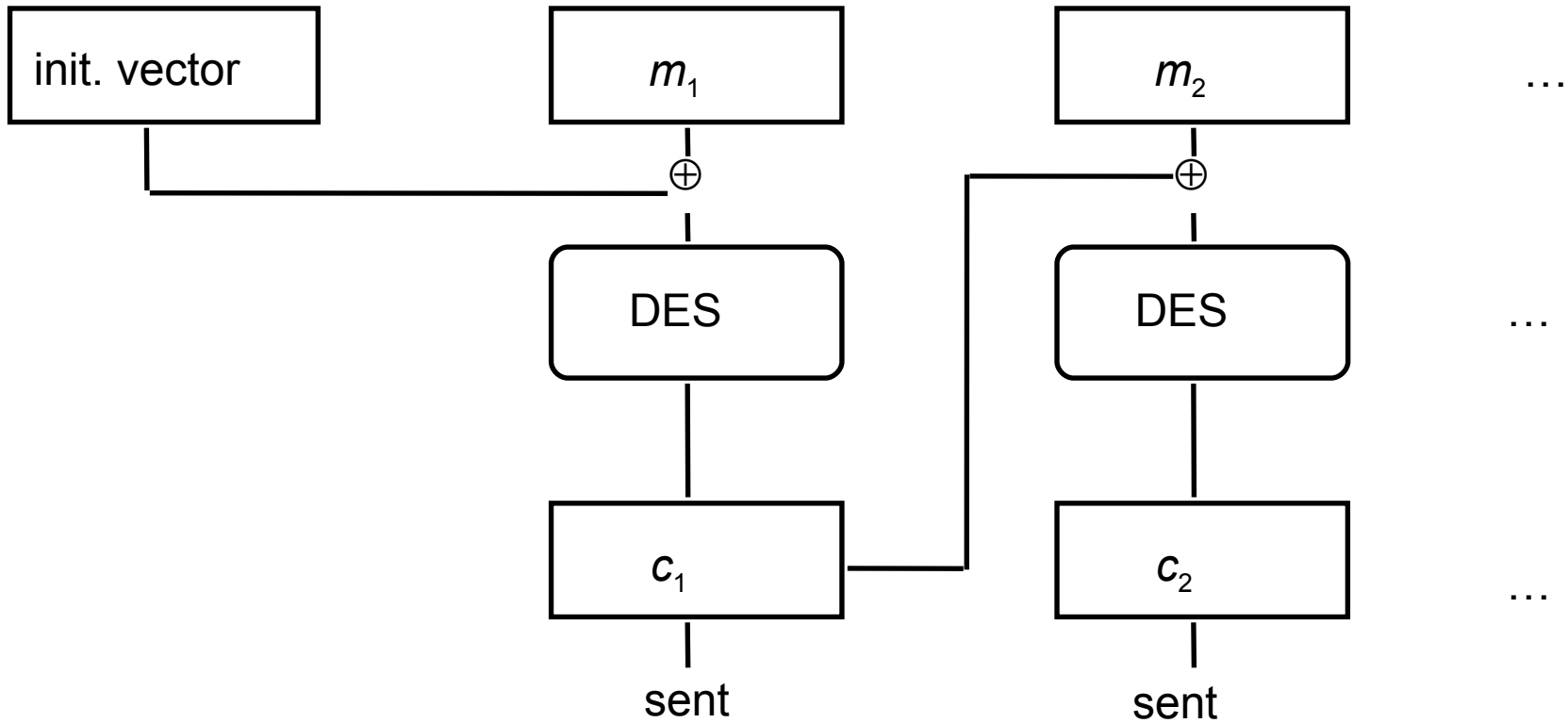
Block Encryption Modes

- Described in section 7.2.2 of the Handbook of Applied Cryptography
<http://www.cacr.math.uwaterloo.ca/hac/about/ch>
- Electronic Codebook (ECB)
- Cipher Block Chaining (CBC)
- Output Feedback (OFB)
- Counter
- Cipher Feedback (CFB)

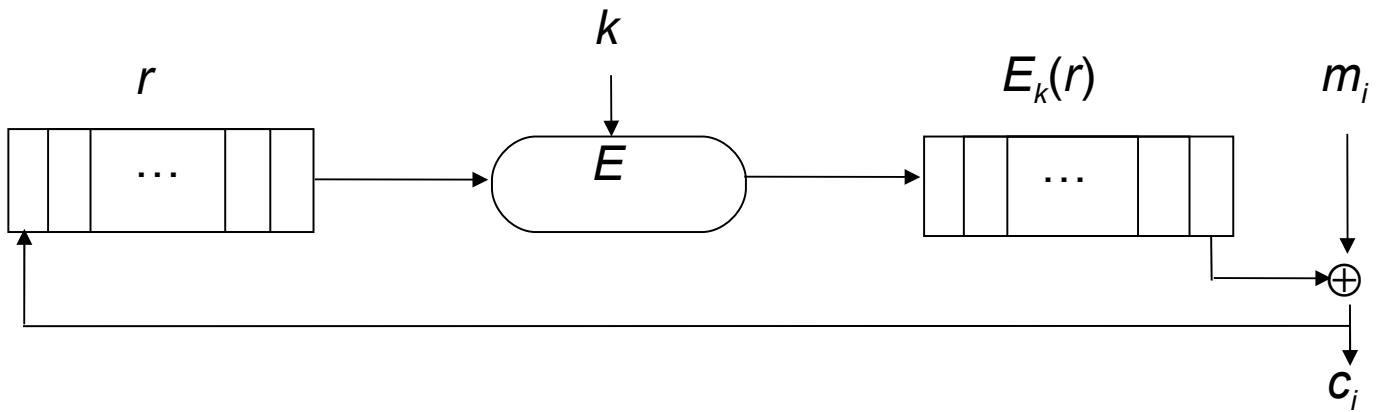
Mode ?



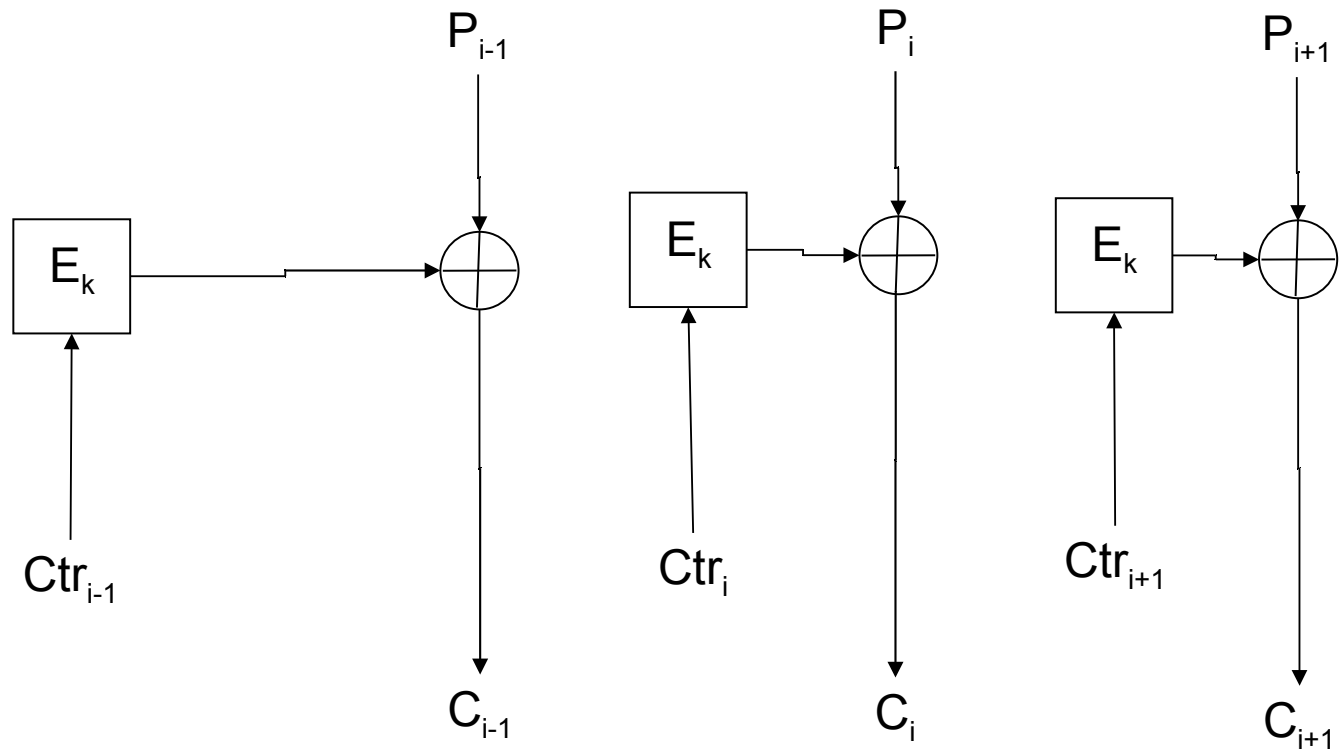
Mode ?



Mode ?



Mode ?



Multiple Encryptions

- Double Encryption doesn't gain much
 - Meet-in-the-middle
 - Both decrypt and encrypt with test key
 - Save both and check against the other for middle values as you check new keys

Public/Asymmetric Encryption

- Two keys
 - One key public, eases some bootstrap issues
- Based on “hard problems”
 - RSA – factoring composites of large primes
 - Diffie Hellman – computing discrete logarithms
- Know equations for RSA and DH
 - What values are public and what are private
- Be able to compute with calculator for small values
 - Divide and Conquer exponentiation

Cryptographic hashes

- Difference from regular checksums
- Keyed and keyless
 - When is each appropriate
- Brute force attack
 - Find another message with the same hash value
- Birthday attack
- Standard algorithms
 - SHA, MD5, block ciphers in CBC mode
- HMAC to make keyless hash keyed

Key Management

- Long lived vs session keys
- Randomness and pseudo random
- Basic key distribution
 - Trusted third party, public key
- Certificates
 - Hierarchical and web of trust
- Digital signatures
 - Several reasons why it is bad to encrypt first

Key management

- Key storage
- Key escrow
 - Should be integrated in to the user's crypto system, authenticated to access escrow system, time bounded message access on unescrow
 - ESS/Clipper example

Good luck!