

Exam 1 Review

CS461/ECE422 Fall 2010

Exam guidelines

- A single page of supplementary notes is allowed
 - 8.5x11. Both sides. Write as small as you like.
- Closed book
- No calculator
- 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 during normal lecture time in 1310 DCL
- You will be given 50 minutes to complete the exam.

Topics

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

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
 - Qualitative uses relative rankings instead of absolute numbers

Security Policy

- Defines what needs to be done, not how
 - How is the mechanism or control
- Organizational or natural language policies
 - Read and identify components in an organizational policy or standard
- Hierarchy of policy languages from natural language to formal specifications to configurations

Historical Ciphers

- Transposition
 - Rail cipher/N-columnar transposition
- Substitution
 - Caesar, Vigenere, book, one-time pad, enigma
- Language-based statistical attacks
 - Character frequency analysis
 - N-gram frequency analysis

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

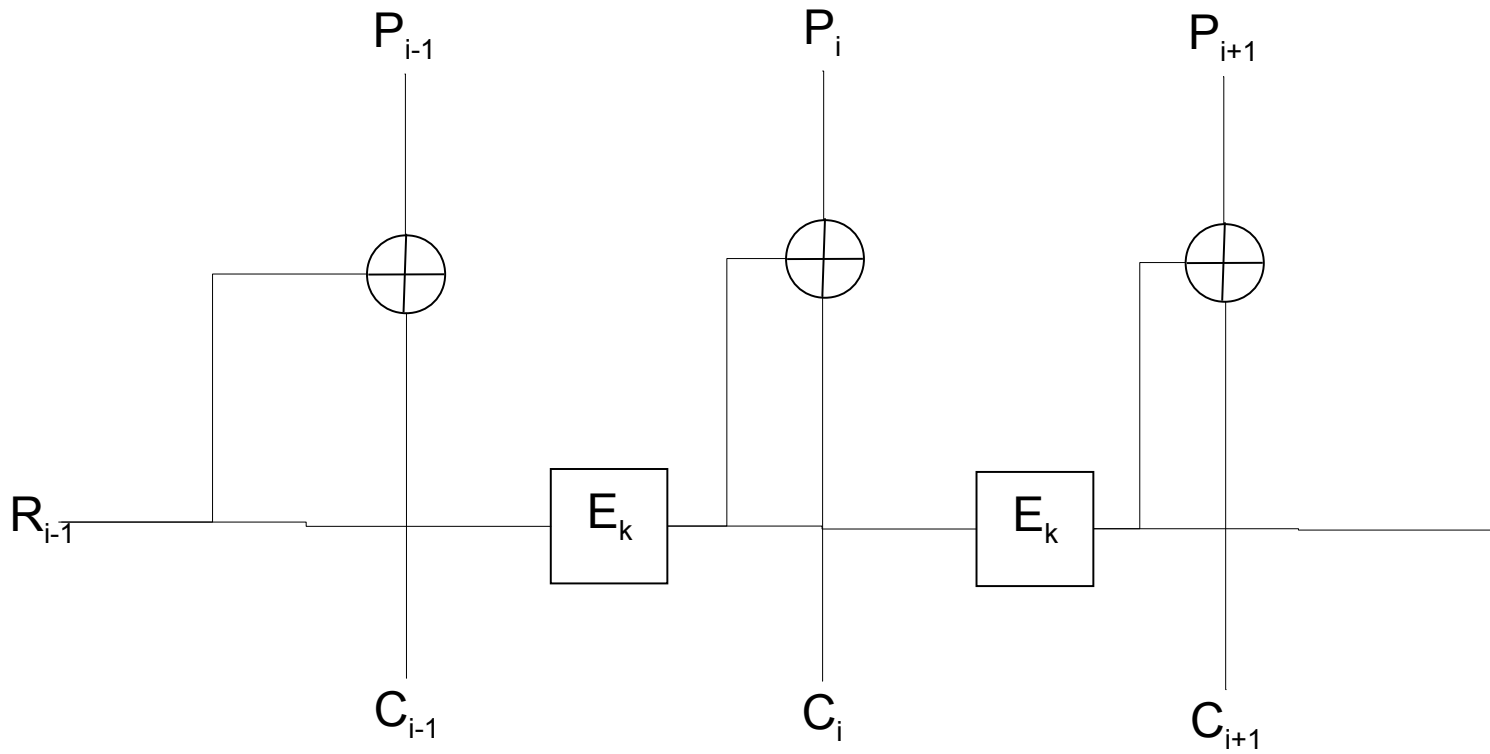
Block Encryption Modes

- Described in text and section 7.2.2 of the Handbook of Applied Cryptography

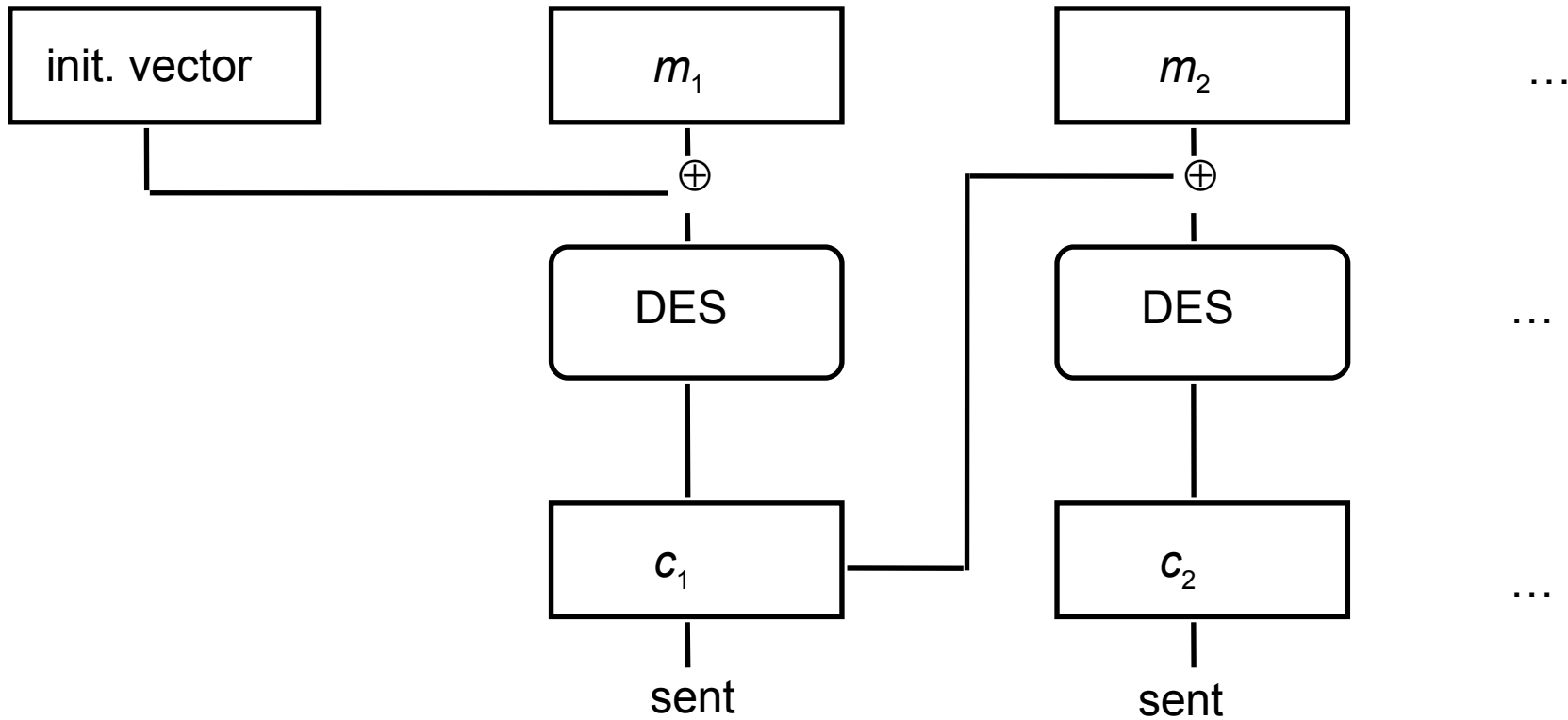
<http://www.cacr.math.uwaterloo.ca/hac/about/chap7>

- Electronic Codebook (ECB)
- Cipher Block Chaining (CBC)
- Output Feedback (OFB)
- Counter
- Cipher Feedback (CFB)

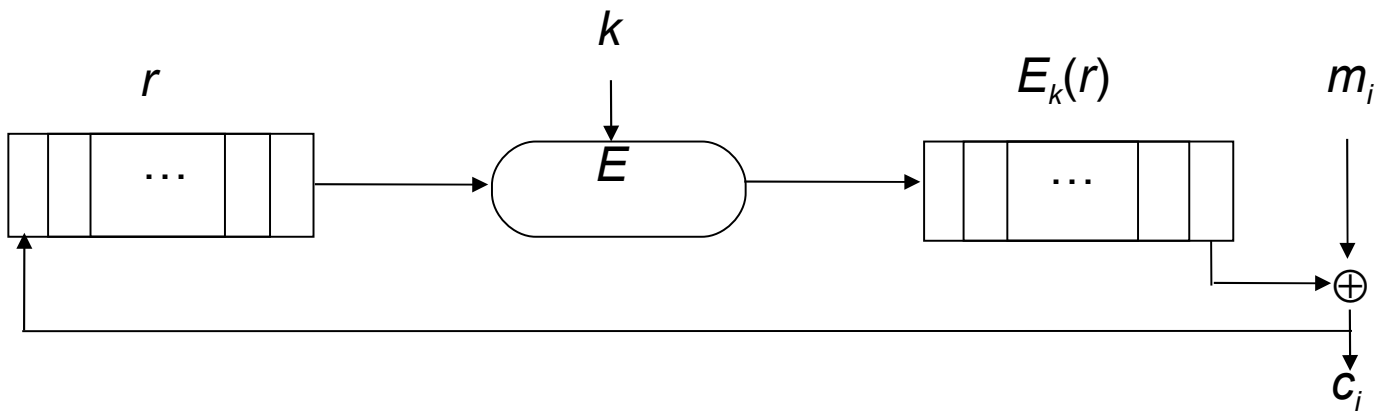
Mode ?



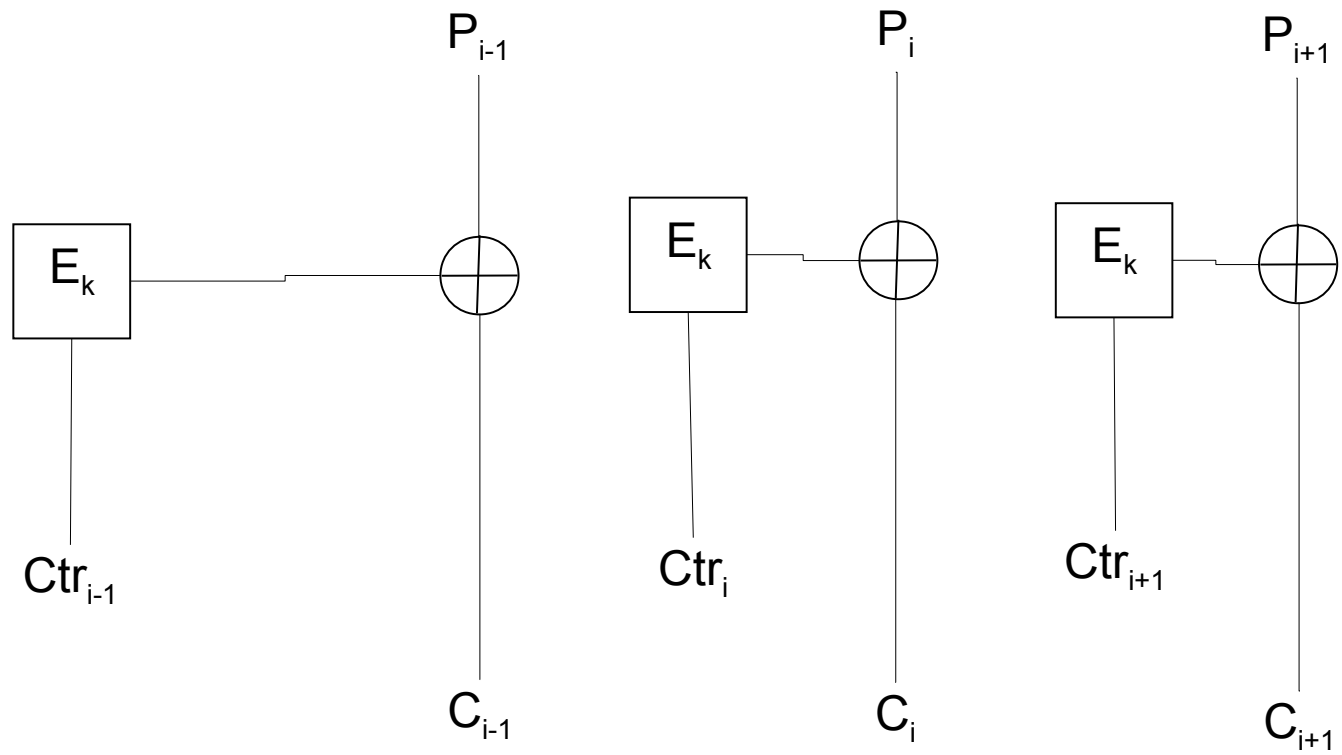
Mode ?



Mode ?



Mode ?



Other key generation techniques

- Physical randomness
- Linear Feedback Shift Registers
- Nonlinear Feedback Shift Registers

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

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
 - Kerberos slides in deck, but hidden
- Certificates
 - Hierarchical and web of trust
- Digital signatures
 - Several reasons why it is bad to encrypt first

Key management

- Key storage
- Key recovery
- 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

Authentication

- Establish ID
 - What you know
 - What you have
 - What you are
 - Where you are
- Spent a lot of time on passwords
 - On line vs off line attacks
 - Salt
 - Anderson's formula
- Challenge Response
- Biometrics

Good luck!