Modes of Operation

Raj Jain
Washington University in Saint Louis
Saint Louis, MO 63130
Jain@cse.wustl.edu

Audio/Video recordings of this lecture are available at :

http://www.cse.wustl.edu/~jain/cse567-06/

1. Modes of Operation: ECB, CBC, OFB, CFB, CTR
2. Privacy+Integrity
3. DES Attacks
4. 3DES and its design

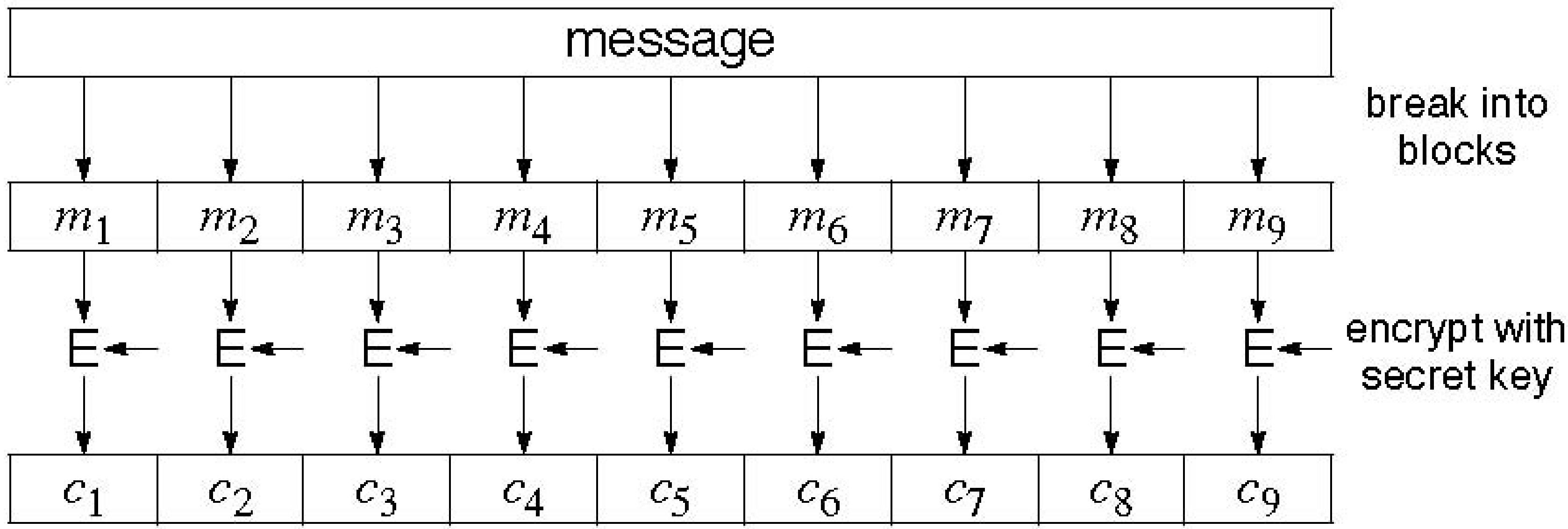
Ref: Chapter 4 of textbook.

Modes of Operation

1. Electronic Code Book (ECB)
2. Cipher Block Chaining (CBC)
3. Cipher Feedback Mode (CFB)
4. Output Feedback Mode (OFB)
5. Counter Mode (CTR)

1. Electronic Code Book (ECB)

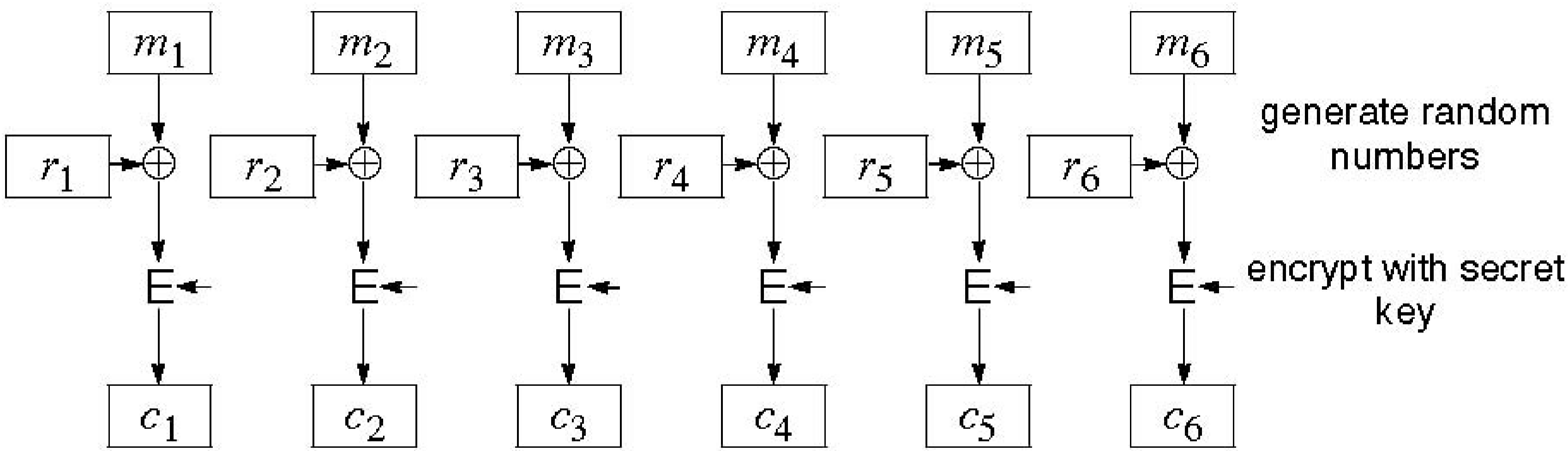
- Each block is independently encoded



- Problem:
  - Identical Input $\Rightarrow$ Identical Output
  - Can insert encoded blocks

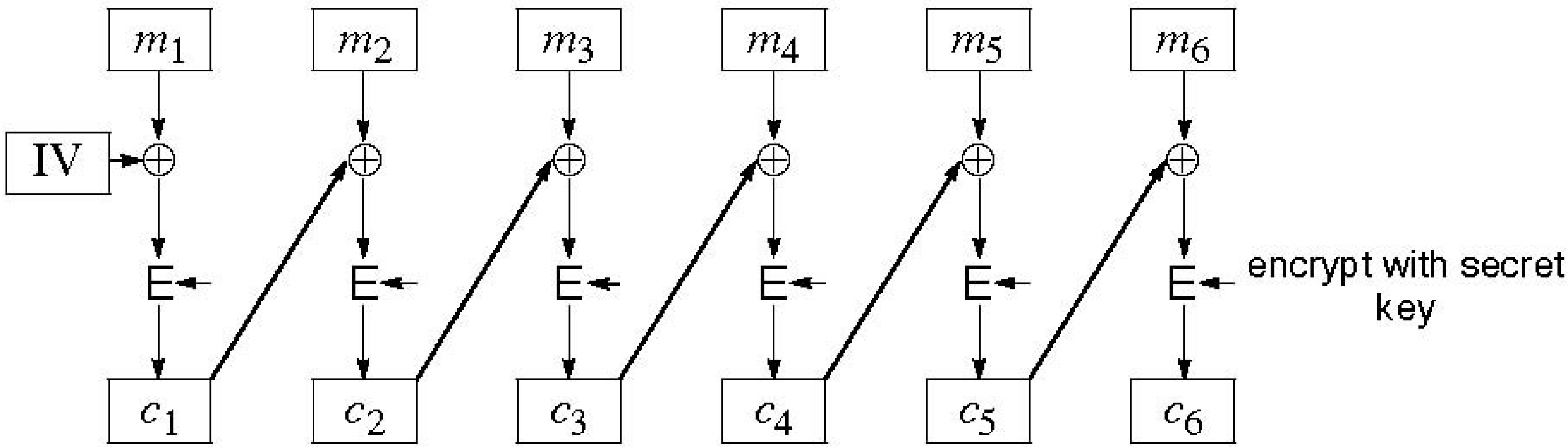
Cipher Block Chaining (CBC)

- Add a random number before encoding



CBC (Cont)

- Use C_i as random number for i+1



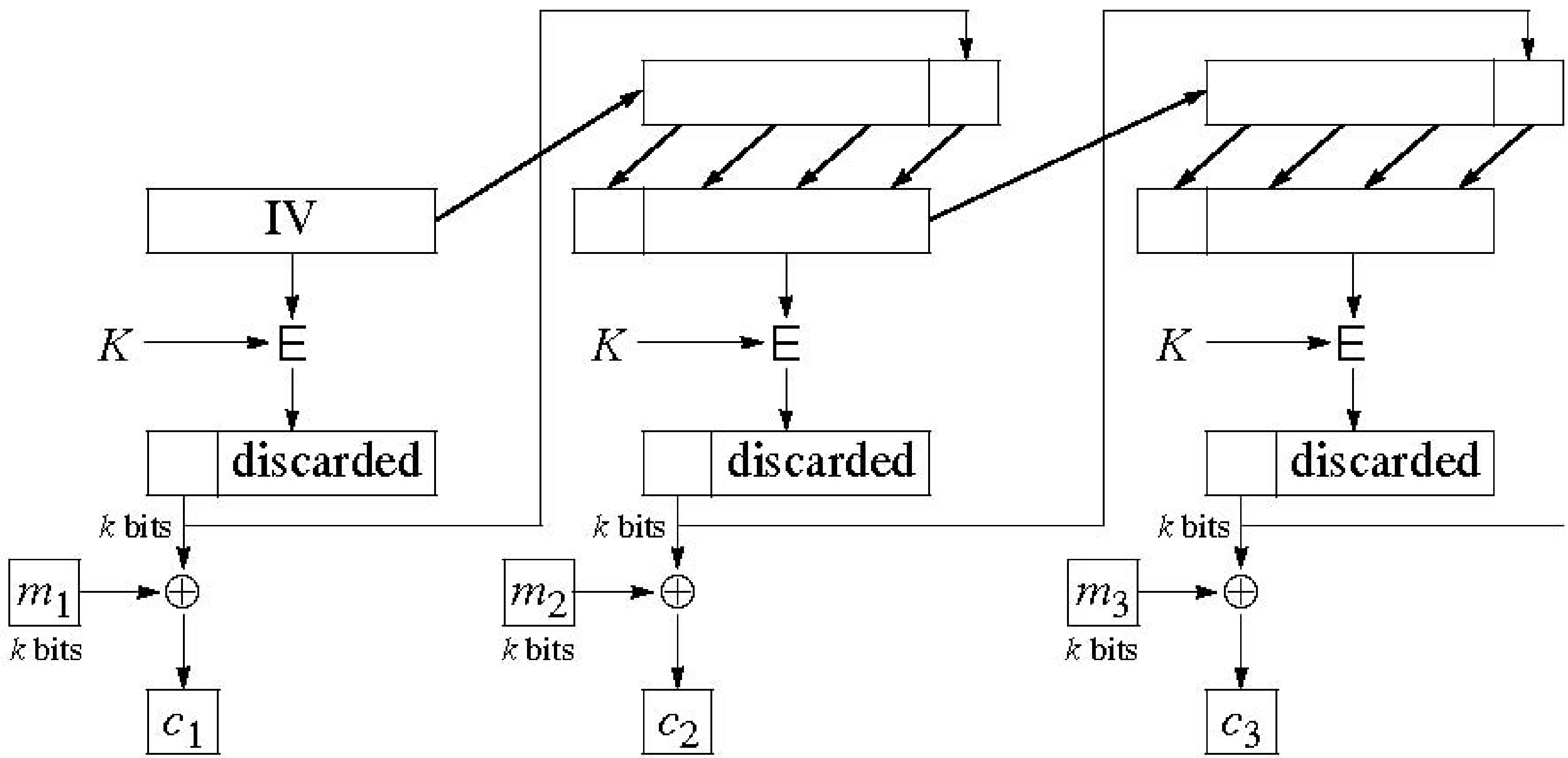
- Need Initial Value (IV)
- If no IV, then one can guess changed blocks
- Example: Continue Holding, Start Bombing

CBC (Cont)

- Attack 1: Change selected bits in encrypted message
  - Garbled text not detected by computers
- Attack 2: Attacker knows plain text and cipher text. Can change plain text.
  - 32-bit CRC may not detect. 64-bit CRC may be better.

k-Bit Output Feedback Mode (OFB)

- IV is used to generate a stream of blocks
- Stream is used a one-time pad and XOR'ed to plain text

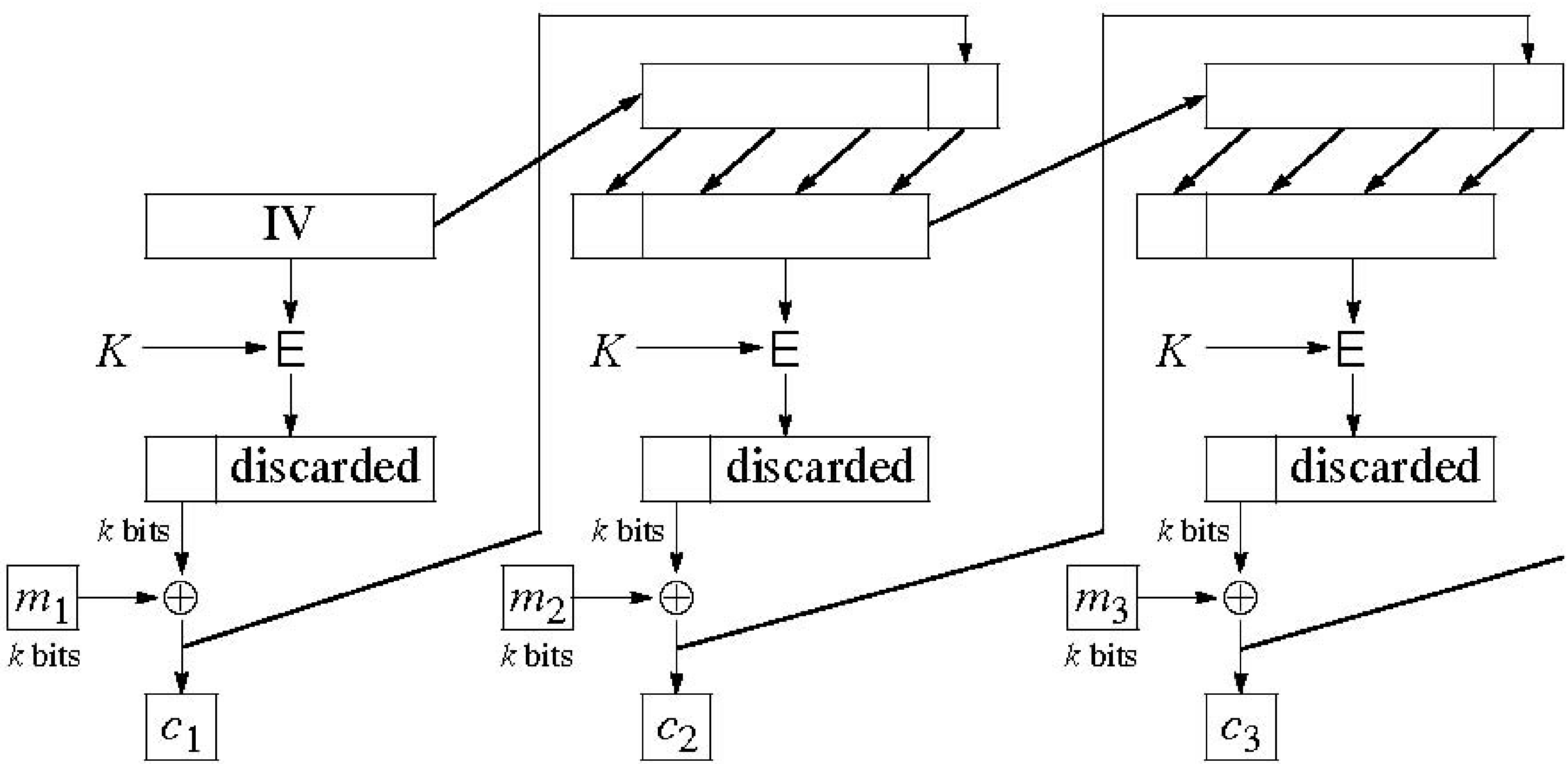


OFB (Cont)

- Advantages:
  - Stream can be generated in advance
  - 1-bit error in transmission affects only one bit of plain text
  - Message can be any size
  - All messages are immediately transmitted
- Disadvantage: Plain text can be trivially modified
- Only left-most k-bits of the block can be used

k-Bit Cipher Feedback Mode (CFB)

- Key Stream blocks use previous block as IV
- k-bits of encoded streams are used to generate next block

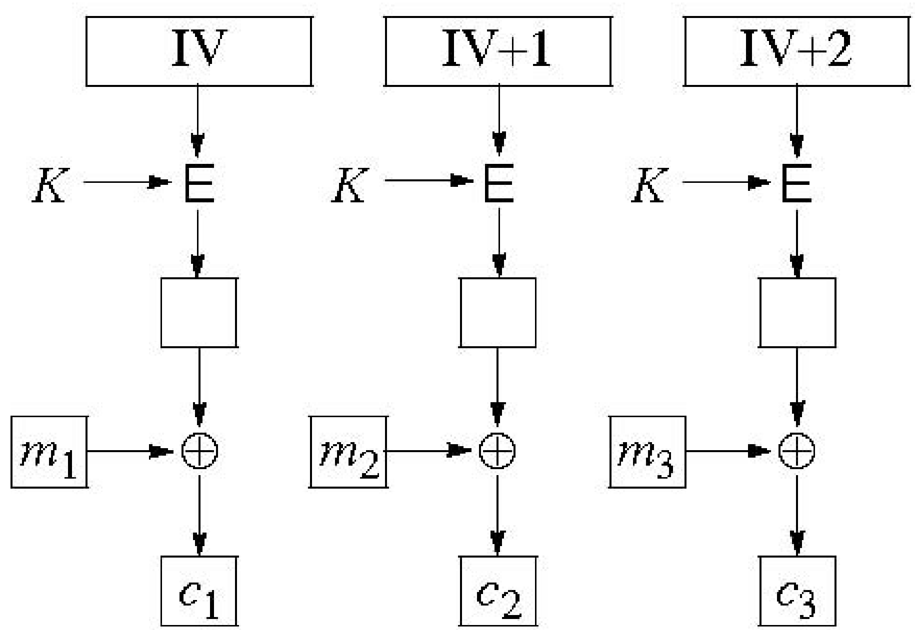


CFB (Cont)

- Stream cannot be generated in advance.
- In practice, k=8 bit or 64 bit
- If a byte is added or deleted, that byte and next 8 bytes will be affected
- No block rearranging effect

Counter Mode (CTR)

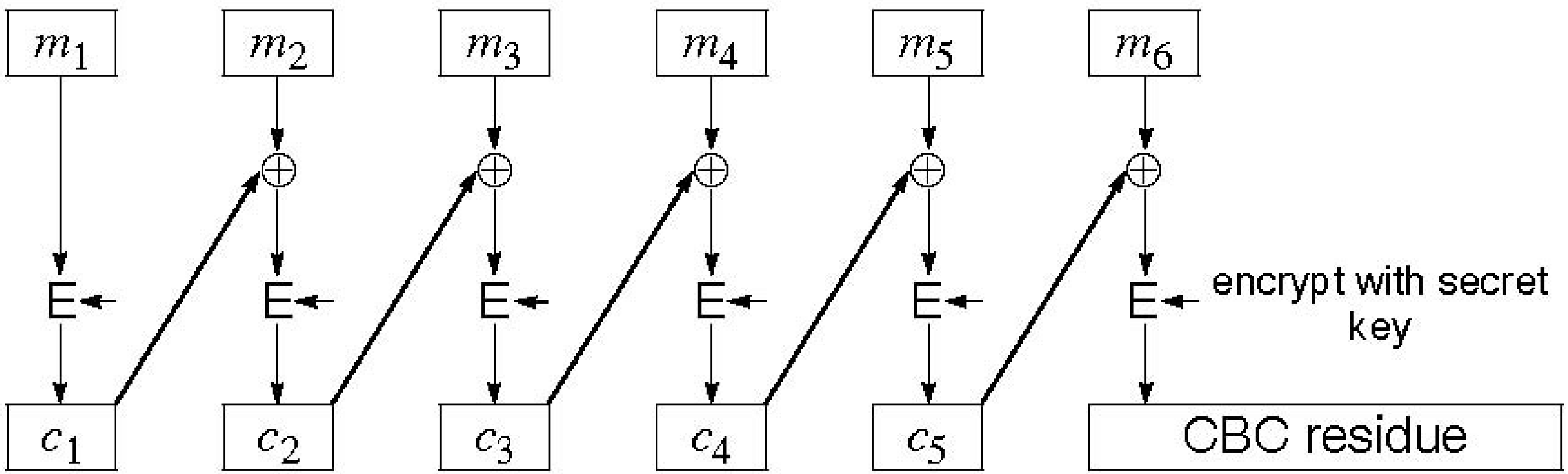
- If the same IV and key is used again,
  - Xor of two encrypted messages = Xor of plain text
- IV is incremented and used to generated one-time pad



- Advantage: Pre-computed

Message Authentication Code (MAC)

- Cryptographic checksum or Message Integrity Code (MIC)
- CBC residue is sent with plain text



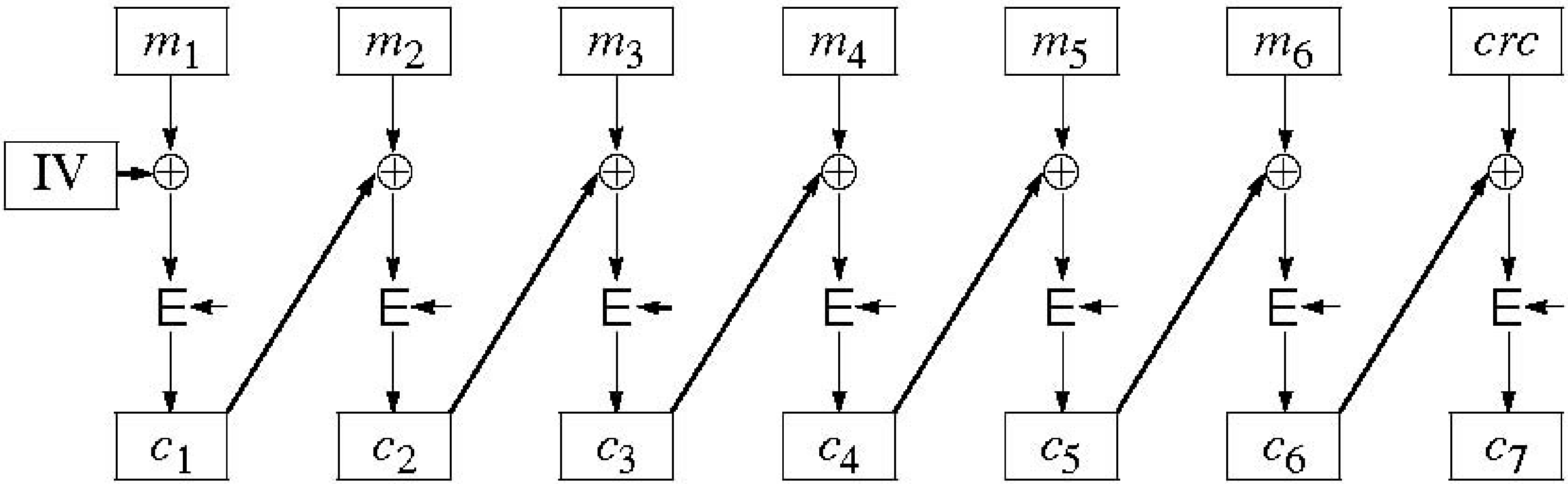
Weak and Semi-Weak Keys

- Recall that 56-bit DES key is divided in two halves and permuted to produce C0 and D0
- Keys are weak if C0 and D0 (after permutation) result in:
  - All 0's
  - All 1's
  - Alternating 10 or 01
- Four possibilities for each half $\Rightarrow$ 16 week keys

Privacy + Integrity

- Can't send encrypted message and CBC residue.

1. Use strong CRC
2. Use CBC residue with another key.



  - The 2nd CBC can be weak, as in Kerberos.
  - Kerberos uses K+F0F0…F0F0 as the 2nd key.

Privacy + Integrity (Cont)

3. Use hash with another key. Faster than encryption.
4. Use Offset Code Book (OCB), http://www.cs.ucdavis.edu/~rogaway/papers/draft-krovetz-ocb-00.txt

MISTY1

- Block cipher with 128 bit keys
- With 4 to 8 rounds. Each round consists of 3 sub-rounds.
- Secure against linear and differential cryptanalysis
- Named after the inventors: Matsui Mitsuru, Ichikawa Tetsuya, Sorimachi Toru, Tokita Toshio, and Yamagishi Atsuhiro
- A.k.a. Mitsubishi Improved Security Technology
- Recommended for Japanese government use. Patented
- Described in RFC 2994
- Ref: http://en.wikipedia.org/wiki/MISTY1

KASUMI

- Selected by 3GPP
- 64-bit block cipher with 128 bit key
- A variant of MISTY1
- Needs limited computing power
- Works in real time (voice)
- KASUMI with counter mode and output feedback modes. This algorithm is known as f8.

GSM Encryption

- Three stream ciphers: A5/1, A5/2, A5/3
- Description of A5/1 and A5/2 were never released to public but were reverse engineered and broken
- A5/3 is based KASUMI

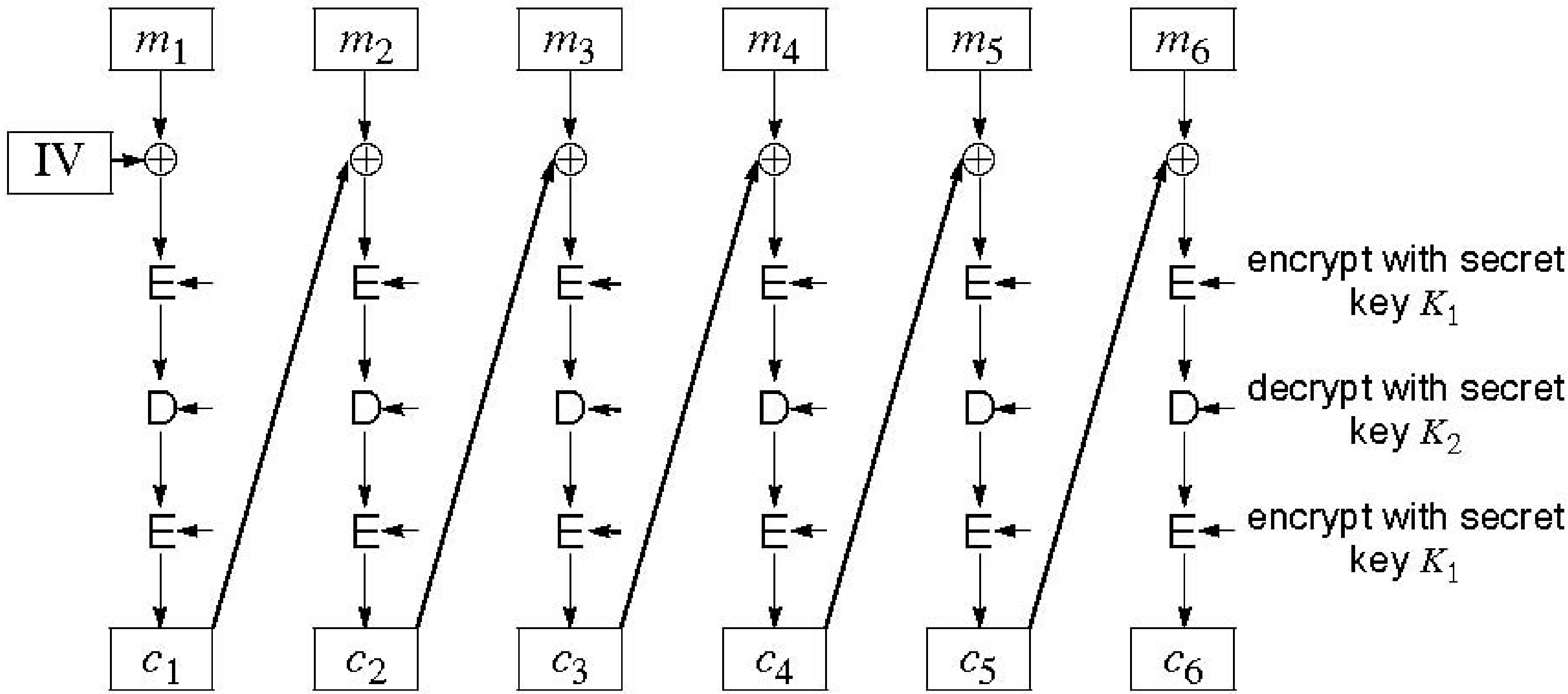
DES Attacks

- 1997 RSA Lab set a prize of $10k
- Curtin and Dolske used combined power of Internet computers to find the key using a brute force method.
- 1998 Electronic Frontier Foundation (EFF) showed that a $250k machine could find any DES key in max 1 week. Avg 3 days.
- 2001 EFF combined the cracker with Internet to crack DES in 1 day.
- Differential Cryptanalysis and Linear cryptanalysis can be used to crack DES
- NIST recommended 3DES

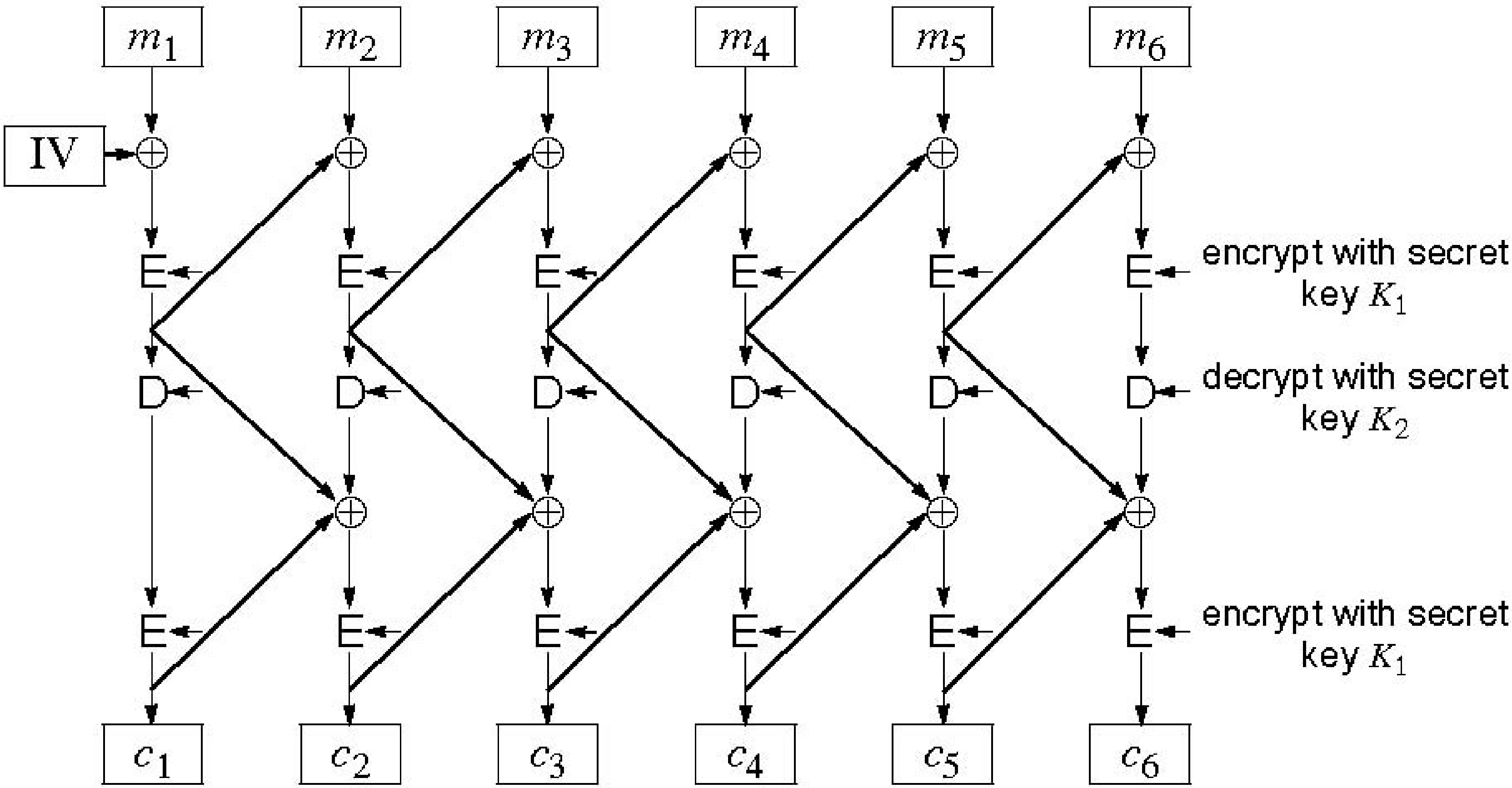
3DES

- $c = e_{k1}(d_{k2}(e_{k3}(m)))$
- $m = d_{k3}(e_{k2}(d_{k1}(c)))$
- k1 and k2 should be independent but k3 can be independent or k3=k1
- k3 = k1 results in 112 bit strength

CBC: Outside vs. Inside



CBC: Outside vs. Inside (Cont)



Key 3DES Design Decisions

1. 3 stages
2. Two keys
3. E-D-E
4. CBC Outside

1. Why not 2DES?

- ek1(ek2(m))
- 2DES is only twice as secure as DES (57-bit key)
- Suppose you know (m1,c1), (m2,c2), ...
- c1=ek1(ek2(m1))
- dk1(c1)=ek2(m1)
- k1 and k2 can be found by preparing two 2^56 entry tables
- Table 1 contains all possible encryptions of m1.
- Table 2 contains all possible decryptions of c1.
- Sort both tables.
- Find matching entries $\Rightarrow$ potential (k1,k2) pairs
- Try these pairs on (m2, c2), ...

2. Why Only Two Keys?

- k3=k1 is as secure as k3\=k1
- Given (m,c) pairs, it is easy to find 3 keys such that ek1(dk2(ek3(m)))=r
- But finding the keys when k3=k1 is difficult.

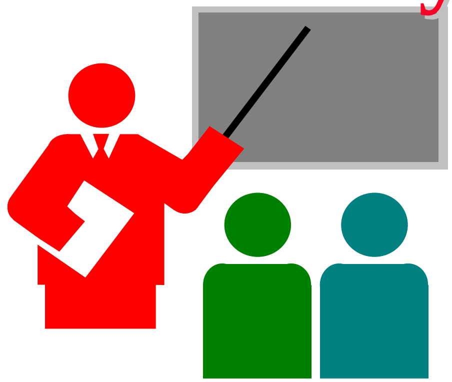
3. Why E-D-E and not E-E-E?

- E and D are both equally strong encryptions.
- With k1=k2, EDE = E
  $\Rightarrow$ a 3DES system can talk to DES by setting k1=k2

4. Why CBC outside?

1. Bit Flipping:
   - CBC Outside: One bit flip in the cipher text causes that block of plain text and next block garbled
     $\Rightarrow$ Self-Synchronizing
   - CBC Inside: One bit flip in the cipher text causes more blocks to be garbled.
2. Pipelining:
   - More pipelining possible in CBC inside implementation.
3. Flexibility of Change:
   - CBC outside: Can easily replace CBC with other feedback modes (ECB, CFB, ...)

Summary



1. To encrypt long messages, we need to use different modes of operation
2. Five modes of operation: ECB, CBC, OFG, CFB, CTR
3. Privacy + Integrity: Use CRC or CBC residue
4. 3DES uses two keys and E-D-E sequence and CBC on the outside.

References

1. C. Kaufman, R. Perlman, and M. Speciner, “Network Security: Private Communication in a Public World,” 2nd Ed, Prentice Hall, 2002, ISBN: 0130460192
2. William Stallings, “Cryptography and Network Security,” 4th Ed, Prentice-Hall, 2006, ISBN:013187316
3. A. W. Dent and C. J. Mitchell, “User’s Guide to Cryptography and Standards,” Artech House, 2005, ISBN:1580535305
4. N. Ferguson and B. Schneier, “Practical Cryptography,” Wiley, 2003, ISBN:047122894X

Homework 6

- Read chapter 4 of the textbook
- Submit answer to Exercise 4.4
- **Exercise 4.4**: What is a practical method of finding a triple of keys that maps a *given* plain text to a given cipher text using EDE?
  Hint: 1. You have only one (m, c) pair
  2. Worst case is to have 3 nested loops for trying all k1, k2, k3 $\Rightarrow 2^{64} \times 2^{64} \times 2^{64} = 2^{192}$ steps but requires storing only 1 intermediate result.
  3. How can you reduce the number of steps using more storage for intermediate results.