Block ciphers (Mode of Encryption)

Hyoungshick Kim

Department of Software

College of Software

Sungkyunkwan University

Application: Storing a file securely

$$M = M_0, M_1, M_2, \ldots, M_{N-1}$$

by a block cipher

$$C = C_0, C_1, C_2, \ldots, C_{N-1}$$

What can attacker learn from captured C?

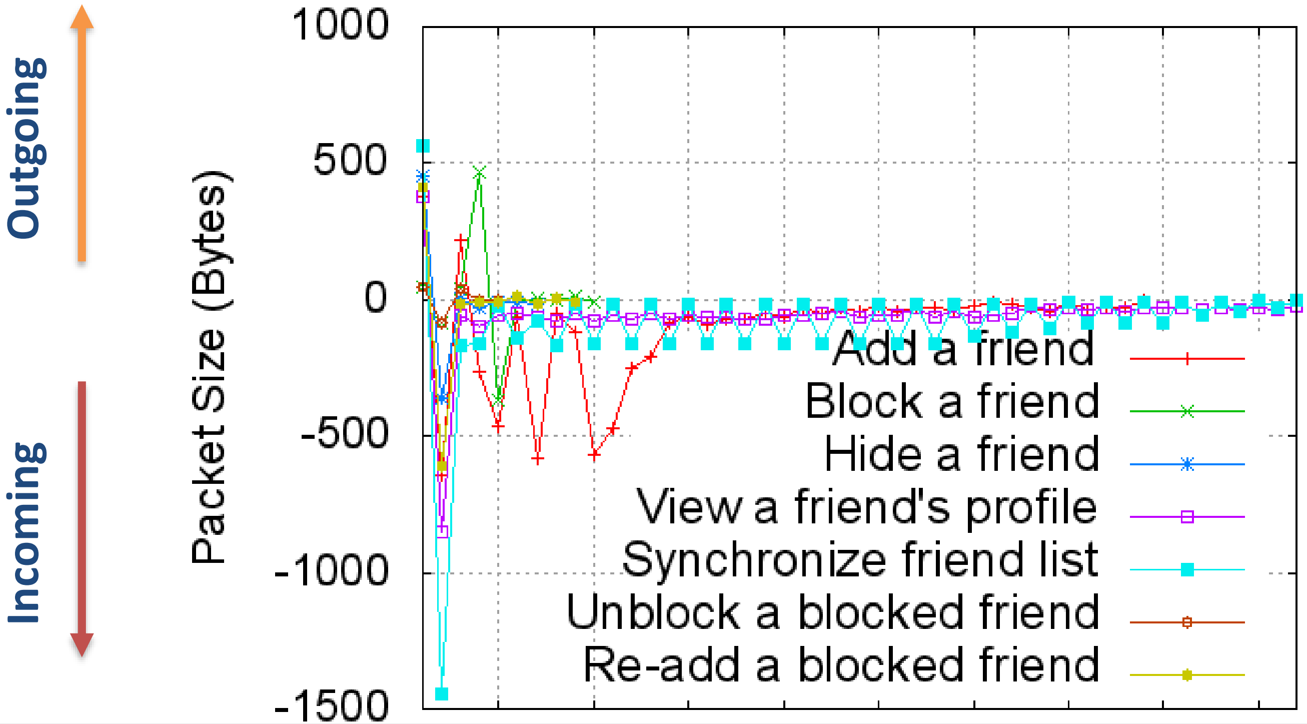
The length of M (i.e., file size)

Which blocks in M are equal

Encryption and plaintext length

- In practice, we use encryption schemes that can encrypt arbitrary-length messages.
- In general, encryption does not hide the plaintext length which might be used for traffic analysis.
- Beware that leaking plaintext length can often lead to problems!
  - Database searches (through the size of responses)
  - For example, user activities in KakaoTalk can be identified with about 99.7% accuracy.

Traffic analysis in KakaoTalk

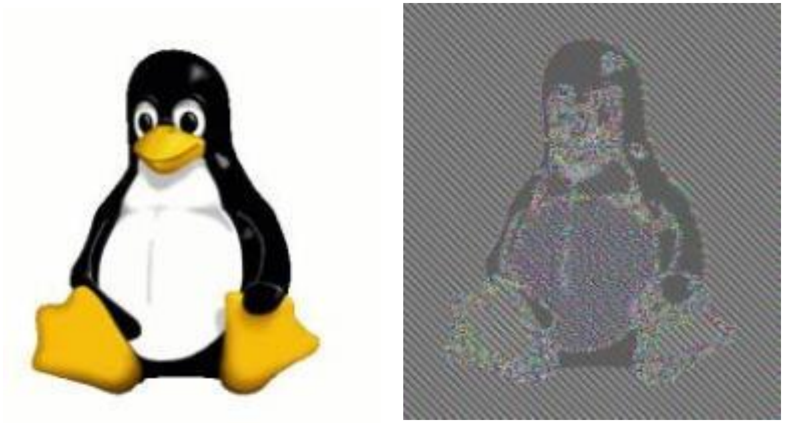


User activities in KakaoTalk can be identified through traffic analysis with about 99.7% accuracy.

"Encryption Is Not Enough: Inferring user activities on KakaoTalk with traffic analysis", WISA 2015

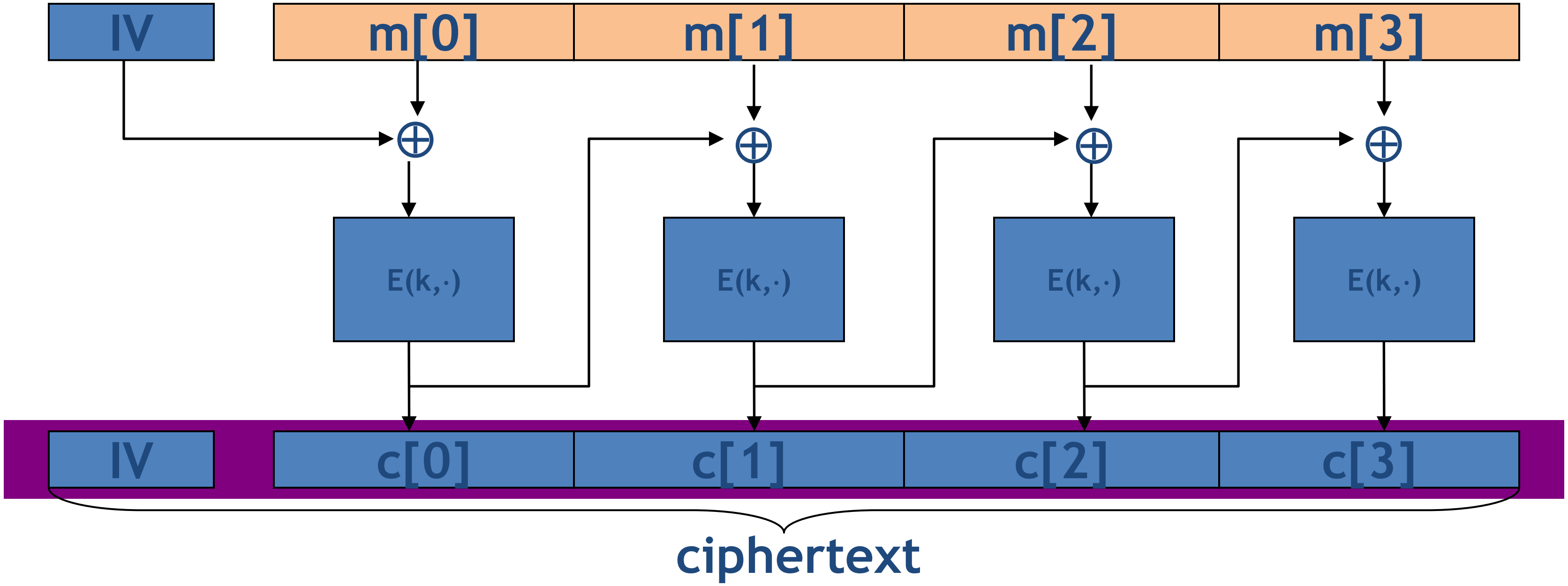
Modes of operation - ECB

ECB – electronic codebook – mode just encrypts a block at a time



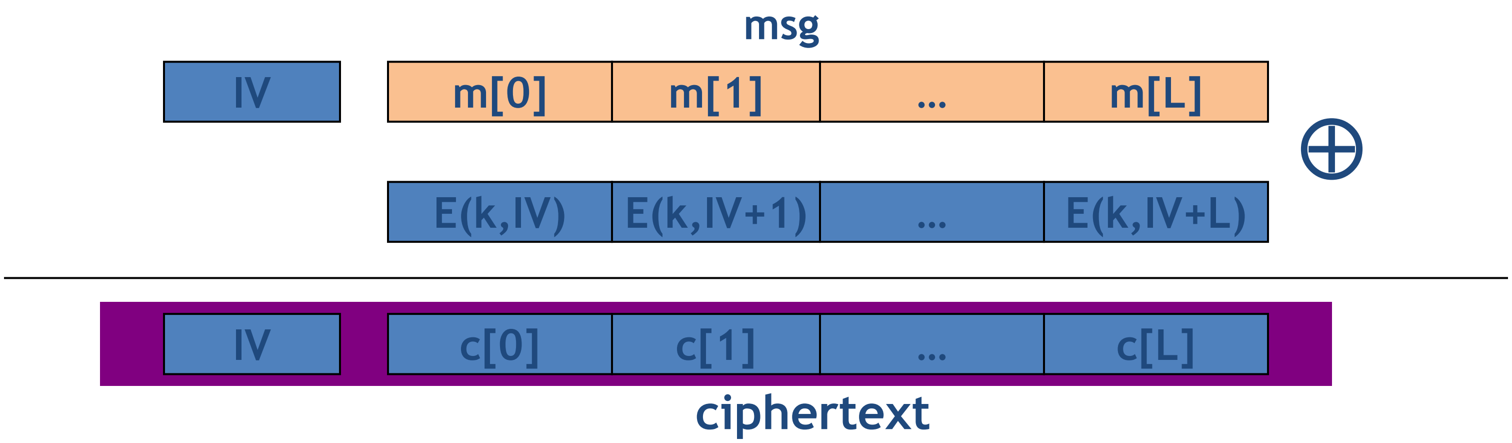
Patterns can still be fairly obvious!

Modes of operation - CBC



- Cipher block chaining (CBC) was the traditional mode for bulk encryption
- If attacker can predict IV, CBC is not secure against Chosen Plaintext Attack.
  - Attacker uses M XOR IV instead of M.
- Error propagates

Modes of operation - CTR



- Counter mode (encrypt a counter to get keystream)
- Unlike CBC, one encryption per block – and parallelizable!
- Random access is possible
- Efficient for software and hardware
- Used in various protocols (e.g., SSH, IPSEC …)

Quiz

Q. Suppose Alice forgets the value she used for IV (initialization vector), has ciphertext (encrypted with CBC) and key. Can she recover plaintext m?

1. No
2. [✓ Almost everything except m[0]]
3. Almost everything except m[0] and m[1]
4. Can only recover m[n-1]

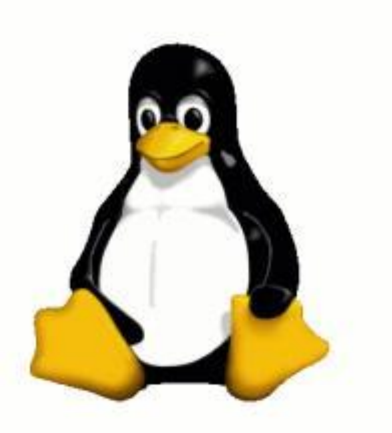
Quiz

Q. If Alice wants to quickly encrypt a large file by using many processors, which mode is preferred?

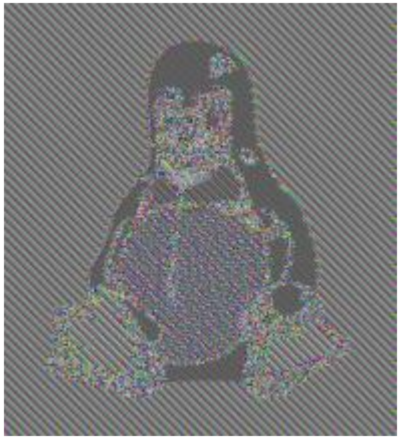
1. CBC or CTR
2. ECB
3. CBC

● 4. CTR

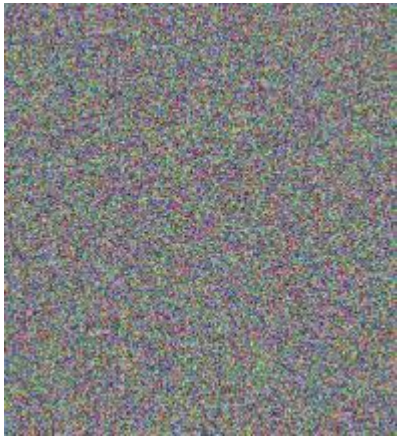
Revisit the previous example



Original



Encrypted with ECB



Encrypted with CBC/CTR

Questions?

Sungkyunkwan
Campus
Social
Institute
Building
Global
Joseon
located
Engineering
Education
University
Sciences
campus
Graduate
Professors
English
Confucian
Zone
Korea
Seoul
Natural
Suwon
School
Korean
university
established
edit
constructed
Advanced
Humanities
lecturers
Science
schools
Administration
Academic
ASLE-Korea
city
also
two
four
capital
Business
Samsung
now
Hall
Course
University's
establishment
Anniversary
symbol
trees
heart
Language
Nanotechnology
Literature
original
campuses
storeys
modern
Location
Research
philosophy
management
Institution
Japanese
considered
Dynasty
Humanity
expansion
Undergraduate
one
years
taught
former
new
Higher
levels
Technology
foreign
College
classes
600th
International
abides
March
South
Sungkyun
attend
university's