Computer Security

Attack Models in Cryptography

Hyoungshick Kim

Department of Software

College of Software

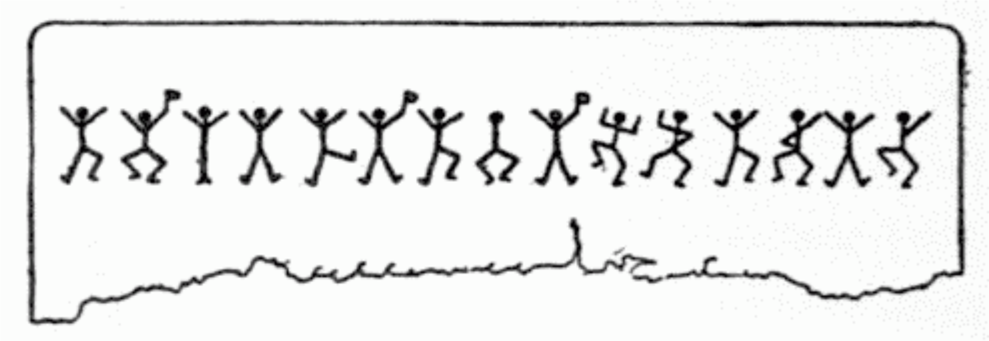
Sungkyunkwan University

Attack models

- Ciphertext only
- Known plaintext
- Chosen plaintext (CPA)
- Chosen ciphertext (CCA1, CCA2)
- Exhaustive key search (in honey encryption)

Ciphertext only attack

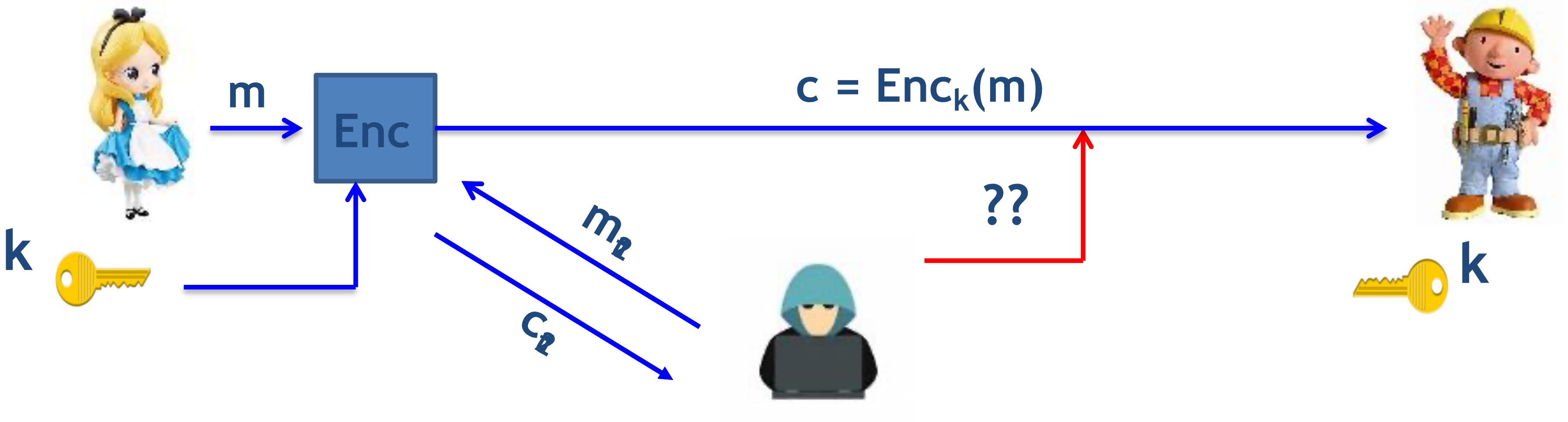
- Attacker has access to a set of ciphertexts
- Goal: to determine the underlying plaintexts
- Passive/Eavesdropper in nature
- Guess-and-check
- Frequency analysis



Known plaintext attack

- Attacker has the ciphertext and some samples of plaintext
- Apply the known plaintext to the ciphertext to help decryption
- Preferred over ciphertext-only

Chosen Plaintext Attack (CPA)



$(m_1, c_1), (m_2, c_2), \ldots, (m_t, c_t)$: $c_i = \mathrm{Enc}_k(m_i)$

>> Adversary influences the honest parties to get encryption of plaintexts (using the same key) of its choice

>> Adv's Goal: to determine the plaintext encrypted in a new ciphertext

Is CPA realistic ?

- How can an attacker influence parties to encrypt messages of its choice (using the same key)?

- Consider a secure hardware with secret-key embedded

  >> Often used in military applications

- An insider may have access to the hardware (not the key)

  >> Can choose messages of its choice and get their encryptions

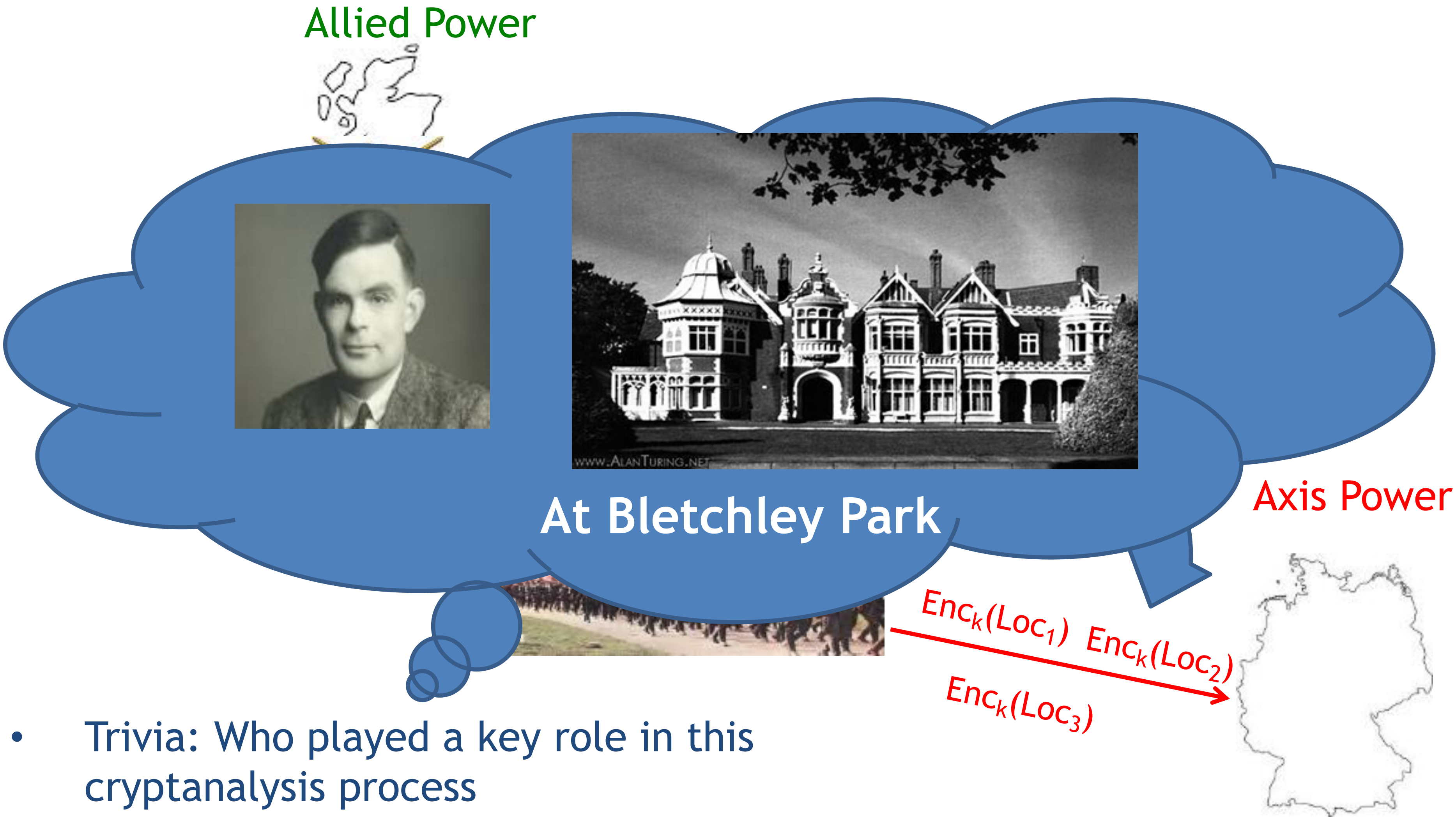
Encryption Oracle

Midway islands (non-CPA secure)

- American cryptanalysts thought: * = Midway Island
- Americans sent: “Midway is low on water”
- Japanese sent: “* blah blah”
- Americans confirmed that * = Midway Island
- Lesson: Adversaries can influence the message.

CPA shortened WWII by 2-3 Years

- Breaking of German codes by British during WW II



Allied Power

At Bletchley Park

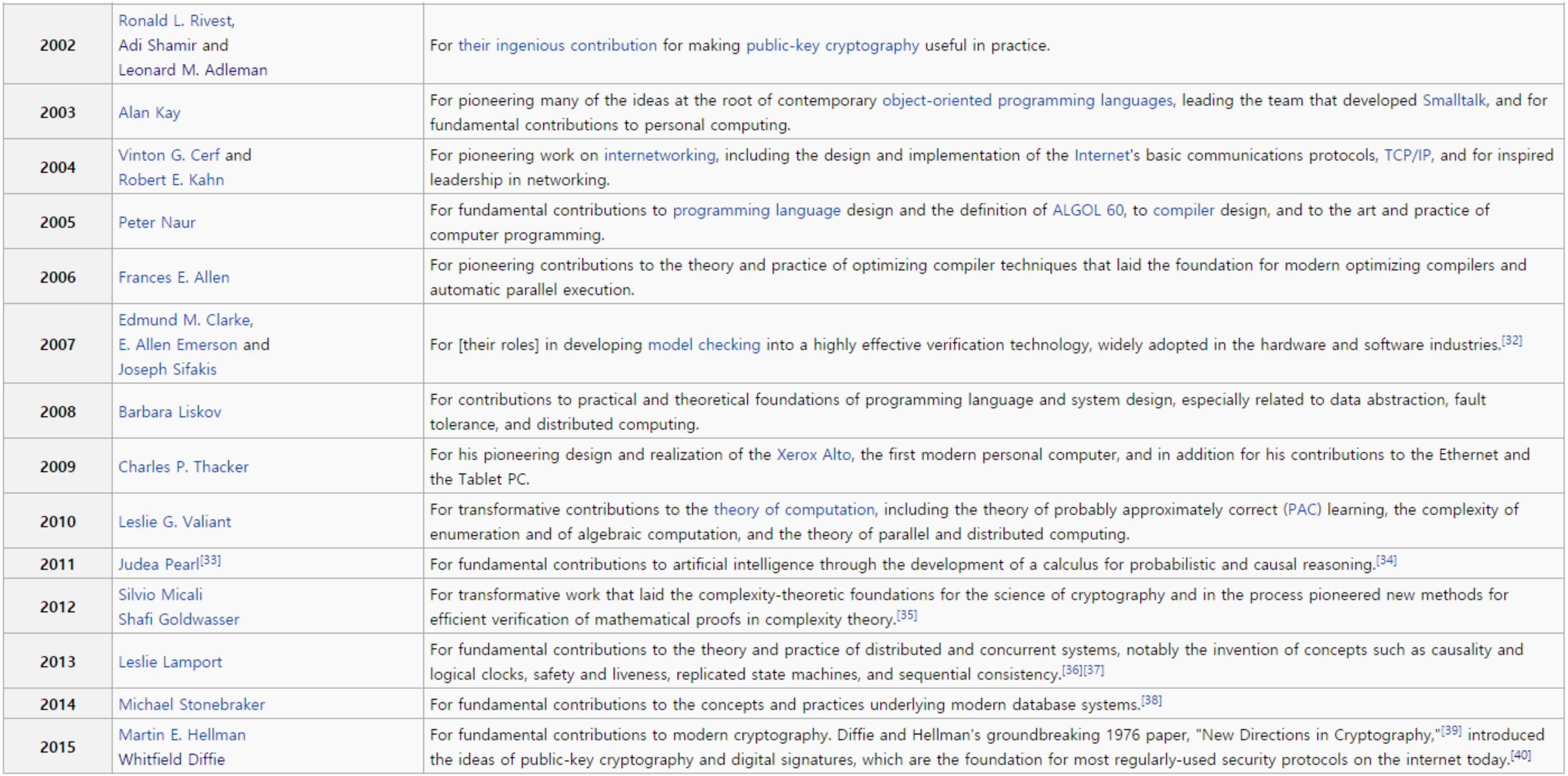
Axis Power

$\mathrm{Enc}_k(\mathrm{Loc}_1)$ $\mathrm{Enc}_k(\mathrm{Loc}_2)$

$\mathrm{Enc}_k(\mathrm{Loc}_3)$

- Trivia: Who played a key role in this cryptanalysis process

ACM Turing award

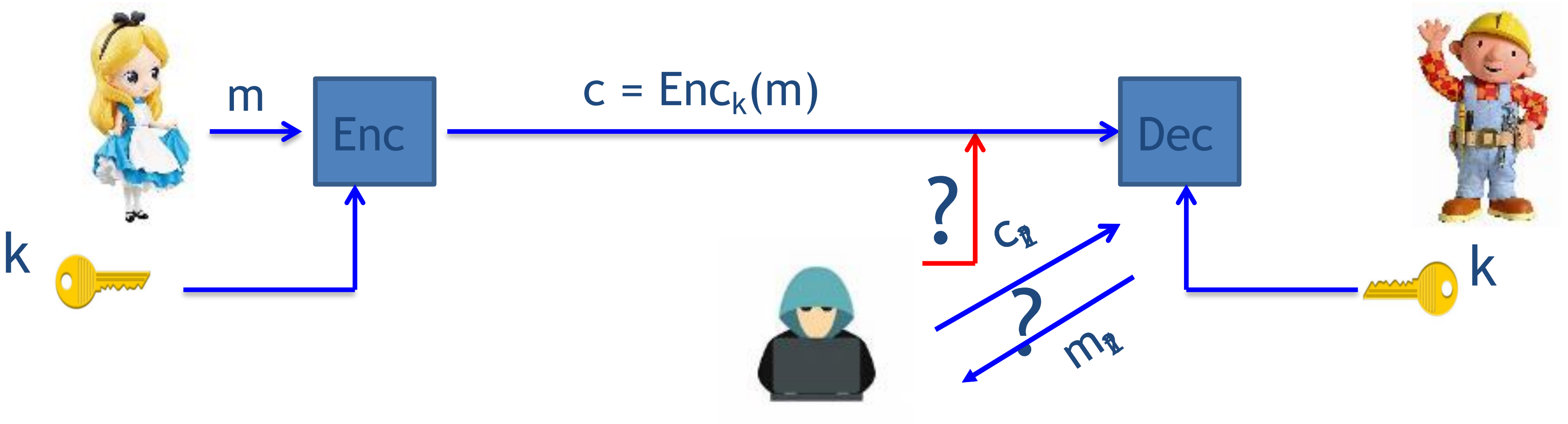


2002	Ronald L. Rivest, Adi Shamir and Leonard M. Adleman	For their ingenious contribution for making public-key cryptography useful in practice.
2003	Alan Kay	For pioneering many of the ideas at the root of contemporary object-oriented programming languages, leading the team that developed Smalltalk, and for fundamental contributions to personal computing.
2004	Vinton G. Cerf and Robert E. Kahn	For pioneering work on internetworking, including the design and implementation of the Internet's basic communications protocols, TCP/IP, and for inspired leadership in networking.
2005	Peter Naur	For fundamental contributions to programming language design and the definition of ALGOL 60, to compiler design, and to the art and practice of computer programming.
2006	Frances E. Allen	For pioneering contributions to the theory and practice of optimizing compiler techniques that laid the foundation for modern optimizing compilers and automatic parallel execution.
2007	Edmund M. Clarke, E. Allen Emerson and Joseph Sifakis	For [their roles] in developing model checking into a highly effective verification technology, widely adopted in the hardware and software industries.[32]
2008	Barbara Liskov	For contributions to practical and theoretical foundations of programming language and system design, especially related to data abstraction, fault tolerance, and distributed computing.
2009	Charles P. Thacker	For his pioneering design and realization of the Xerox Alto, the first modern personal computer, and in addition for his contributions to the Ethernet and the Tablet PC.
2010	Leslie G. Valiant	For transformative contributions to the theory of computation, including the theory of probably approximately correct (PAC) learning, the complexity of enumeration and of algebraic computation, and the theory of parallel and distributed computing.
2011	Judea Pearl[33]	For fundamental contributions to artificial intelligence through the development of a calculus for probabilistic and causal reasoning.[34]
2012	Silvio Micali Shafi Goldwasser	For transformative work that laid the complexity-theoretic foundations for the science of cryptography and in the process pioneered new methods for efficient verification of mathematical proofs in complexity theory.[35]
2013	Leslie Lamport	For fundamental contributions to the theory and practice of distributed and concurrent systems, notably the invention of concepts such as causality and logical clocks, safety and liveness, replicated state machines, and sequential consistency.[36][37]
2014	Michael Stonebraker	For fundamental contributions to the concepts and practices underlying modern database systems.[38]
2015	Martin E. Hellman Whitfield Diffie	For fundamental contributions to modern cryptography. Diffie and Hellman's groundbreaking 1976 paper, "New Directions in Cryptography,"[39] introduced the ideas of public-key cryptography and digital signatures, which are the foundation for most regularly-used security protocols on the internet today.[40]

Chosen Ciphertext Attack (CCA)

- Tries to discover the key
- Uses a ciphertext chosen by attacker
- Relies on being able to obtain decrypted plaintext
- Two variations
  - Lunchtime attack (CCA1)
  - Adaptive chosen-ciphertext (CCA2)

Chosen Ciphertext Attack (CCA)

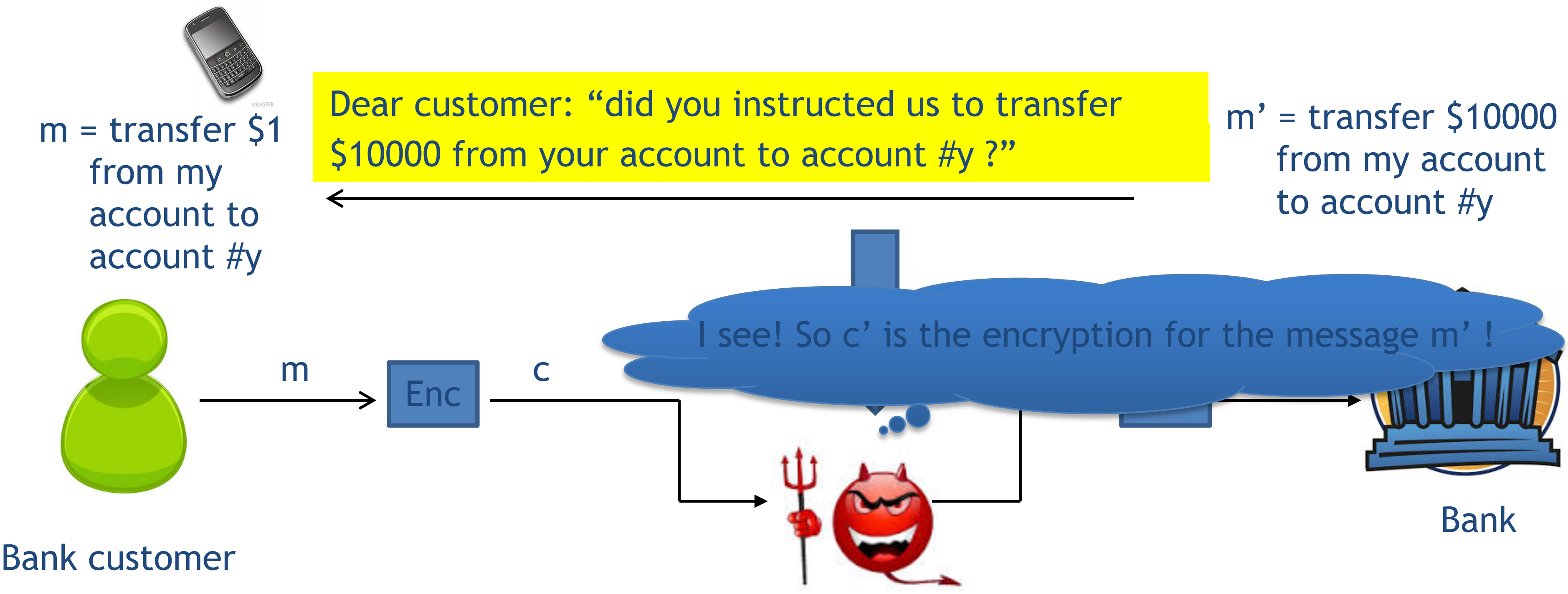


$(c_1, m_1), (c_2, m_2), \ldots, (c_t, m_t): m_i = Dec_k(c_i)$

>> Getting Decryption Oracle (DO) service is much easier than getting Encryption Oracle service

>> Adv's Goal: to determine the plaintext encrypted in a new ciphertext

DO service is practical



m = transfer $1 from my account to account #y

Dear customer: “did you instructed us to transfer $10000 from your account to account #y ?”

m’ = transfer $10000 from my account to account #y

I see! So c’ is the encryption for the message m’ !

Adversary is no longer an eavesdropper, he is active and malicious!!

❑ Similar scenarios:

>> An attacker sends an arbitrary ciphertext c’(for an unknown message) to army headquarters and waits for the ciphertext to be decrypted and observes the behavior/movements of the army --- will give an hint what c’ corresponds to

Lunchtime attack (CCA1)

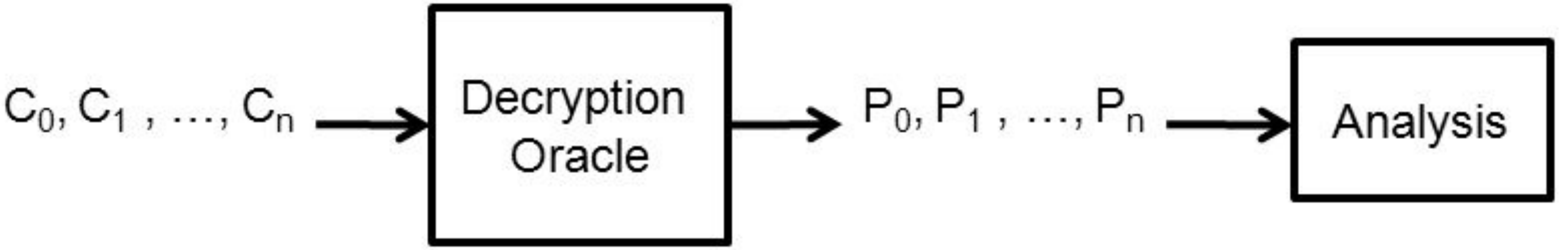
- Attacker can make queries but only up until a certain point
- Attacker cannot adapt queries

Adaptive Chosen-Ciphertext (CCA2)

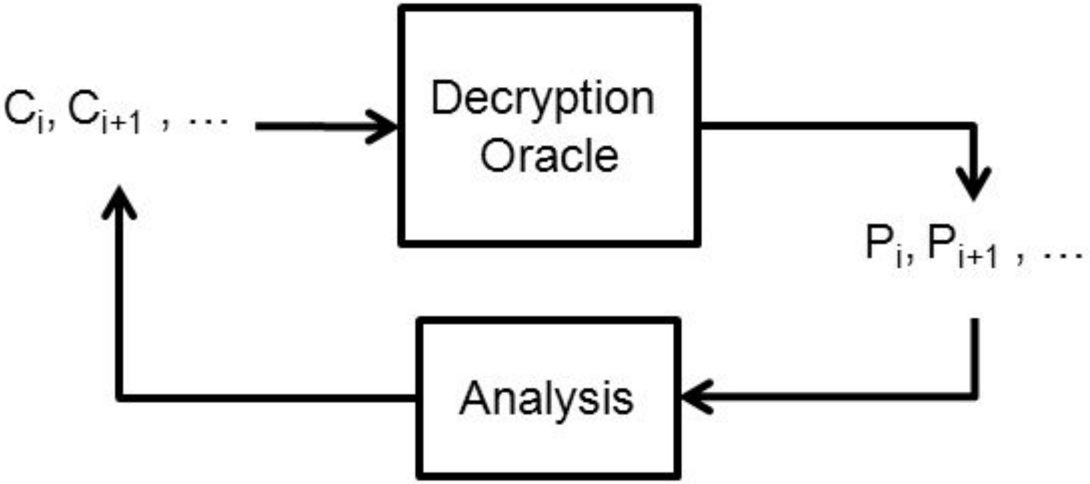
- Similar to lunchtime attack
- Ciphertext is chosen based on the result of the previous queries

CCA1 vs CCA2

- CCA1 (Lunchtime Attack)



- CCA2 (Adaptive Chosen Ciphertext Attack)



Questions?

Sungkyunkwan
Campus
established
Sciences
campus
University
university
Suwon
School
Seoul
Natural
Korean
Graduate
constructed
English
Social
Global
edit
Professors
Confucian
Building
Institute
Humanities
Business
Korea
Zone
Advanced
located
Joseon
Engineering
schools
Science
Administration
Academic
ASLE-Korea
also
lecturers
two
four
Hall
Education
symbol
city
trees
Samsung
now
Anniversary
University's
establishment