Introduction

Cryptography - CS 411 / CS 507

Erkay Savaş

Department of Computer Science and Engineering
Sabancı University

September 19, 2019

Announcements - I

- Textbook
  - Nigel P. Smart. Cryptography Made Simple. Springer, 2016. ISBN 978-3-319-21936-3
- Additional Resources
  - W. Trappe & L. C. Washington. Introduction to Cryptography with Coding Theory, 2nd Edition, Prentice-Hall, 2006. ISBN:0-13-198199-4.
  - C. Paar & J. Pelzl. Understanding Cryptography. Springer 2010. ISBN: 978-3-642-04100-6
  - D. R. Stinson, Cryptography: Theory and Practice, 3rd Edition, Chapman & Hall/CRC, 2006.
  - A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997.

Announcements - II

- Python programming language will be used for homework assignments and term project
  - See
    http://people.sabanciuniv.edu/erkays/lyo/lyo2019.htm
    for basics of Python (in Turkish)
- Python support for number theory and cryptographys
  - https://pypi.python.org/pypi/eulerlib/0.2
  - https://pypi.python.org/pypi/pycrypto
- We will use Google Colab to run your homework assignments
  https://colab.research.google.com
- Check course syllabus
  http://people.sabanciuniv.edu/~erkays/cs507/cs507.htm

Subjects to be Covered

- Classic Ciphers
- Number Theory & Other Math Background
- Stream Ciphers
- Block Ciphers & DES & AES
- Cryptographic Hash Functions
- PKC & RSA & Discrete Logarithm Based Cryptosystems
- Digital Signatures
- Key Management & Distribution
- Elliptic Curve Cryptography
- Zero Knowledge Protocols

Cryptography

- People want/need security, privacy, and trust in the cyberspace.
  - e.g., secure communication over insecure media
- For these, cryptography provides
  - Primitives,
  - Methods,
  - Techniques
  - Protocols, algorithms
- In the past, cryptography is heavily used for military applications (e.g., Caesar cipher)
- Nowadays, cryptography is an essential part of the civilian life

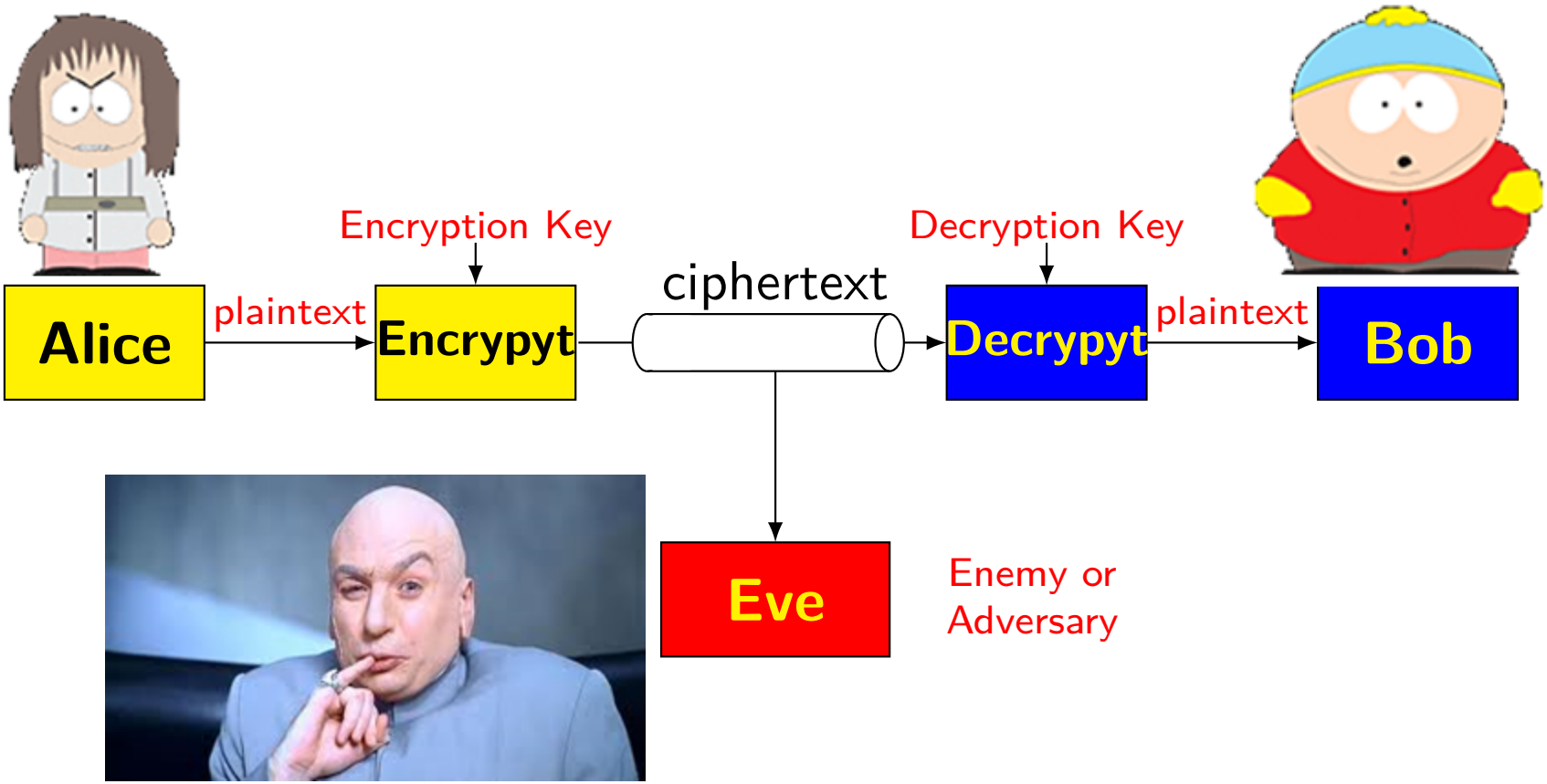
Terminology

- Cryptology
  - All-inclusive term used for the study of secure and trusted systems operating in insecure media and related problems.
- Cryptography
  - The process of designing/constructing/implementing cryptographic systems to realize security and trust in cyberspace which is intrinsically insecure and not-trustable.
- Cryptanalysis
  - The discipline of breaking the cryptographic systems
  - Without a complete understanding of crypto-analytic techniques it is impossible to design good (secure, unbreakable) cryptographic systems
- Coding Theory
  - Deals with representing the information using codes.
  - Compression and error-correction.
  - Recently, it is predominantly associated with error-correcting codes

Aspects of Cryptography

- Modern cryptography heavily depends on
  - Mathematics
  - Digital systems
- Inter-disciplinary study of three fields:
  - Mathematics
  - Computer Science
  - Electrical Engineering
- Other Disciplines
  - coding theory, complexity theory, statistics, physics

Basic Communication Scenario



Eve's Goals

- Passive adversary
  - Read the message
  - Figure out the decryption key and read all messages encrypted with this key
- Active adversary
  1. Modify the contents of the message
     - Bob will think Alice sent the altered message
  2. Impersonate Alice
     - Communicate with Bob who thinks he is communicating with Alice

Attack Methods

1. Ciphertext only
   - Eve has access only to the ciphertext
2. Known Plaintext
   - Eve has pairs of ciphertext and the corresponding plaintext and tries to deduce the key
3. Chosen Plaintext
   - Eve can have a ciphertext corresponding to a sample plaintext which she believes is useful in deducing the key
4. Chosen Ciphertext
   - Eve can have a plaintext corresponding to a sample ciphertext which she believes is useful in deducing the key

Kerckhkoffs' Principle

- Complete knowledge of the algorithm is public
  - While assessing the strength of a cryptosystem, one should always assume that the enemy knows the cryptographic algorithm used
- The security of the system should be based on
  - the quality (strength) of the algorithm, but not its obscurity
  - the key space (or key length)

Symmetric Key Algorithms

- Encryption & decryption keys are known to both
- They are related (if not identical)
  - easy to derive the decryption key once the encryption key is known (and vice versa)
- DES, IDEA, AES (Rijndael)
- A secret must be known (agreed upon) to communicating parties
  - so they can generate encryption and decryption keys
- Key distribution and/or management problem

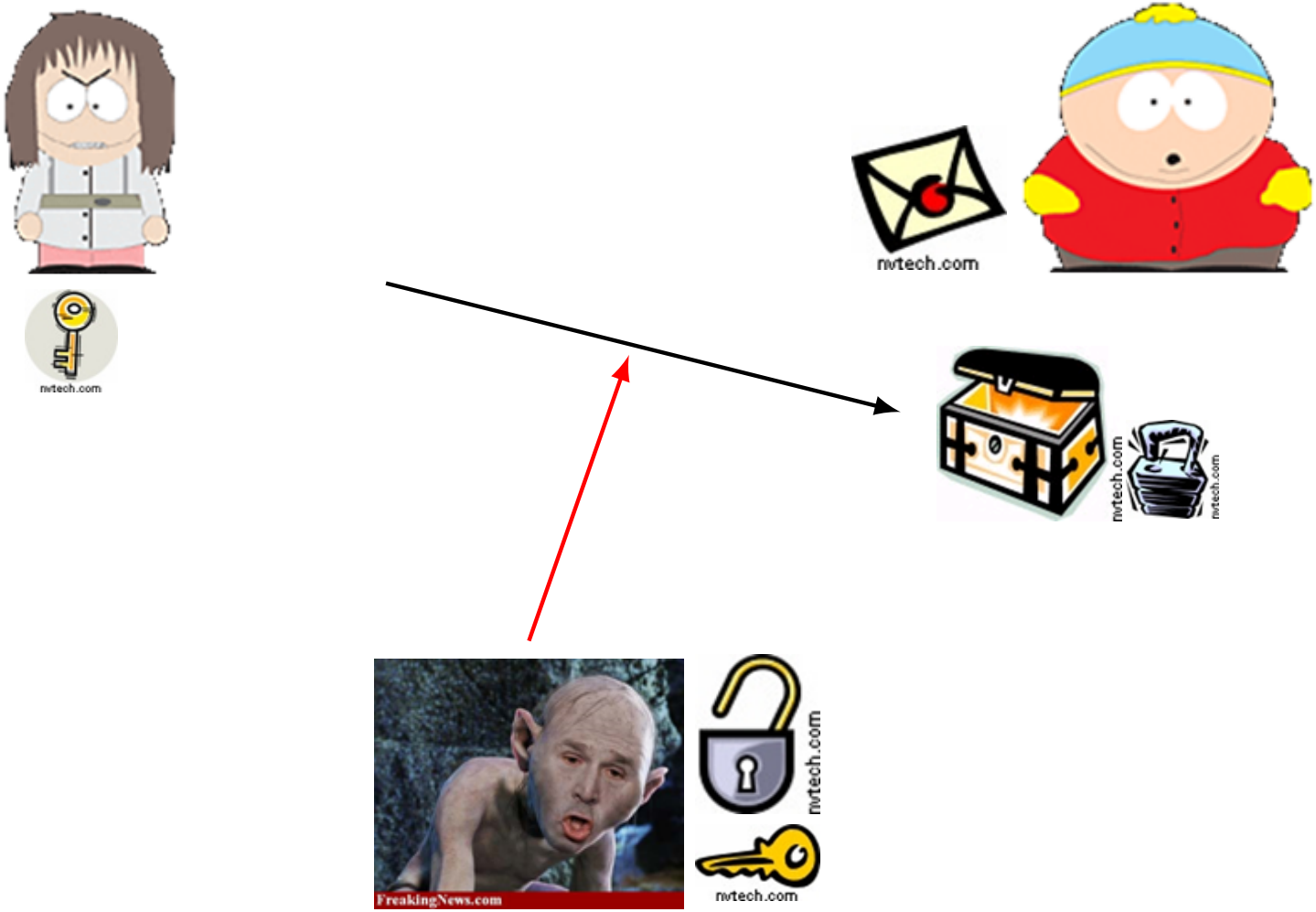
Public Key Cryptosystems - PKC

- Why public key cryptography?
  - Single key $\rightarrow$ security problems
  - Key Distribution and Management is difficult in symmetric cryptosystems (DES, 3DES, IDEA, AES (Rijndael)) over large networks.
  - Electronic signatures
  - Other cryptographic applications such as
    - Key exchange,
    - Secret key derivation,
    - Secret sharing functions,
    - Secure multi-party computations,
    - e-voting,
    - e-cash (e.g., bitcoin)

Fundamentals of PKC

- Each user has a pair of keys which are generated together under a scheme
  - Private key - known only to the owner
  - Public key - known to anyone in the systems with assurance
- Encryption and decryption methods are public
- Encryption
  - Sender encrypts the message by the public key of the receiver
- Decryption
  - Only the receiver can decrypt the message by her/his private key

A Non-Mathematical PKC



Aspects of PKC

- Based on a mathematical problem, which we think, is difficult to solve
  - Computationally infeasible
- Powerful tools with their own problems.
  - Computation and resource intensive operations are involved.
  - Implementation is always a challenge.
  - Much slower than the symmetric key algorithms.
  - PKC is not used for encrypting large amount of data
- Example PKCs
  - RSA,
  - DL,
  - Elliptic curve cryptosystems, IBE
  - Lattice-based cryptosystems

Key Length 1/2

- Kerckhkoffs' principle,
  - the strength (security) of cryptosystems based on two important properties:
    - the quality of the algorithm
    - the key length
- The quality of a cryptosystems is hard to measure
  - provable security
- Key length must be sufficiently large
  - An adversary should not be able figure out the key simply by trying all possible keys in the key space, brute-force or exhaustive-search attacks

Key Length 2/2

- DES utilizes 56-bit keys
  - key space is 2^{56} (or approximately 7.2×10^{16})
- Example: Assume there are $2^{100} \approx 10^{30}$ possible keys
  - Further assume we can try 10^{12} keys in a second
  - 3.15×10^7 seconds in a year
  - Takes 3.17×10^{10} years to try out the keys
    - comparable to the predicted lifetime of the universe
  - What about DES?
    - Couple of days with an optimized hardware (cost $\sim$ \$10,000 US)
    - This explains the switch from 56-bit DES to 128-bit AES

Cryptanalyst's Job

- Brute force or (exhaustive search)is the last resort
- In order to reduce the possible keys to try out one takes advantage
  - Weakness in cryptographic algorithm
  - Weakness in the implementation of cryptographic algorithm
- Longer keys do not necessarily improve the security
  - Effective key length is important

Unbreakable Cryptosystems ??

- Practical Security
  - Almost all of the practical cryptosystems are theoretically breakable given the time and computational resources
- Theoretically unbreakable system:
  - One-time-pad
- One-time pad
  - Requires exchanging a key that is as long as the plaintext.
  - However impractical, it is still being used in certain applications which necessitate very high-level security.
  - Its security relies on the condition that keys are generated using "truly random sources"

Main Objectives of Cryptography

- Confidentiality
  - Hiding contents of messages exchanged in a transaction
- Authentication
  - The origin (owner) of a message is correctly identified
- Integrity
  - Only authorized parties are able to modify data and transmitted information
- Non-repudiation
  - Requires that neither of the authorized parties deny the aspects of a valid transaction

Cryptographic Applications

- Digital Signatures
  - allows electronically sign (personalize) the electronic documents, messages and transactions
- Identification
  - is capable of replacing password-based identification methods with more powerful (secure) techniques
- Key Establishment
  - To communicate a key to your correspondent (or perhaps actually mutually generate it with him) whom you have never physically met before
- Secret Sharing
  - Distribute parts of a secret to a group of people who can never exploit it individually

Cryptographic Applications

- E-commerce
  - Secure transactions over an insecure channel like Internet
- E-cash (e.g., Bitcoin)
  - The cash can be sent securely through computer networks
  - The cash cannot be copied and reused
  - The spender of the cash can remain anonymous
  - The transaction can be done offline
  - The cash can be transferred to others
  - A piece of cash can be divided into smaller amounts
- Electronic Voting
- Secure Multi-party Computation