Cryptography and Network Security

Spring 2012
http://users.abo.fi/ipetre/crypto/

Lecture 1: Introduction

Ion Petre
Department of IT, Åbo Akademi University

Motto

"Unfortunately, the technical wizardry enabling remote collaborations is founded on broadcasting everything as sequences of zeros and ones that one's dog wouldn't recognize.

- *What is to distinguish a digital dollar when it is as easily reproducible as the spoken word?*
- *How do we converse privately when every syllable is bounced on a satellite and smeared over an entire continent?*
- *How should a bank know that it really is Bill Gates requesting from his laptop in Fiji a transfer of $10,000,000,000 to another bank?*

Fortunately, the magical mathematics of cryptography can help. Cryptography provides techniques for keeping information secret, for determining that information has not been tampered with, and for determining who authored pieces of information."

Ronald Rivest

Foreword to Handbook of Applied Cryptography

Why do we need cryptography?

- Computers are used by millions of people for many purposes
  - Banking
  - Shopping
  - Tax returns
  - Protesting
  - Military
  - Student records
  - …
- **Privacy** is a crucial issue in many of these applications
- **Security** is to make sure that nosy people cannot read or secretly modify messages intended for other recipients

Security issues

- The world before computers was in some ways much simpler
  - Signing, legalizing a paper would authenticate it
  - Photocopying easily detected
  - Erasing, inserting, modifying words on a paper document easily detectable
  - Secure transmission of a document: seal it and use a reasonable mail carrier (hoping the mail train does not get robbed)
  - One can recognize each other's face, voice, hand signature, etc.
- Electronic world: the ability to copy and alter information has changed dramatically
  - No difference between an "original" file and copies of it
  - Removing a word from a file or inserting others is undetectable
  - Adding a signature to the end of a file/email: one can impersonate it – add it to other files as well, modify it, etc.
  - Electronic traffic can be (and is!) monitored, altered, often without noticing
  - How to authenticate the person electronically communicating with you

Possible adversaries

- Student: to have fun snooping on other people's email
- Cracker: to test out someone's security system, to steal data
- Businessman: to discover a competitor's strategic marketing plan
- Ex-employee: to get revenge for being fired
- Accountant: to embezzle money from a company
- Stockbroker: to deny a promise made to a customer by email
- Convict: to steal credit card numbers for sale
- Spy: to learn an enemy's military or industrial secrets
- Terrorist: to steal germ warfare secrets

- Point to make: making a network or a communication secure involves more than just keeping it free of programming errors
- It involves outsmarting often intelligent, dedicated and often well-funded adversaries

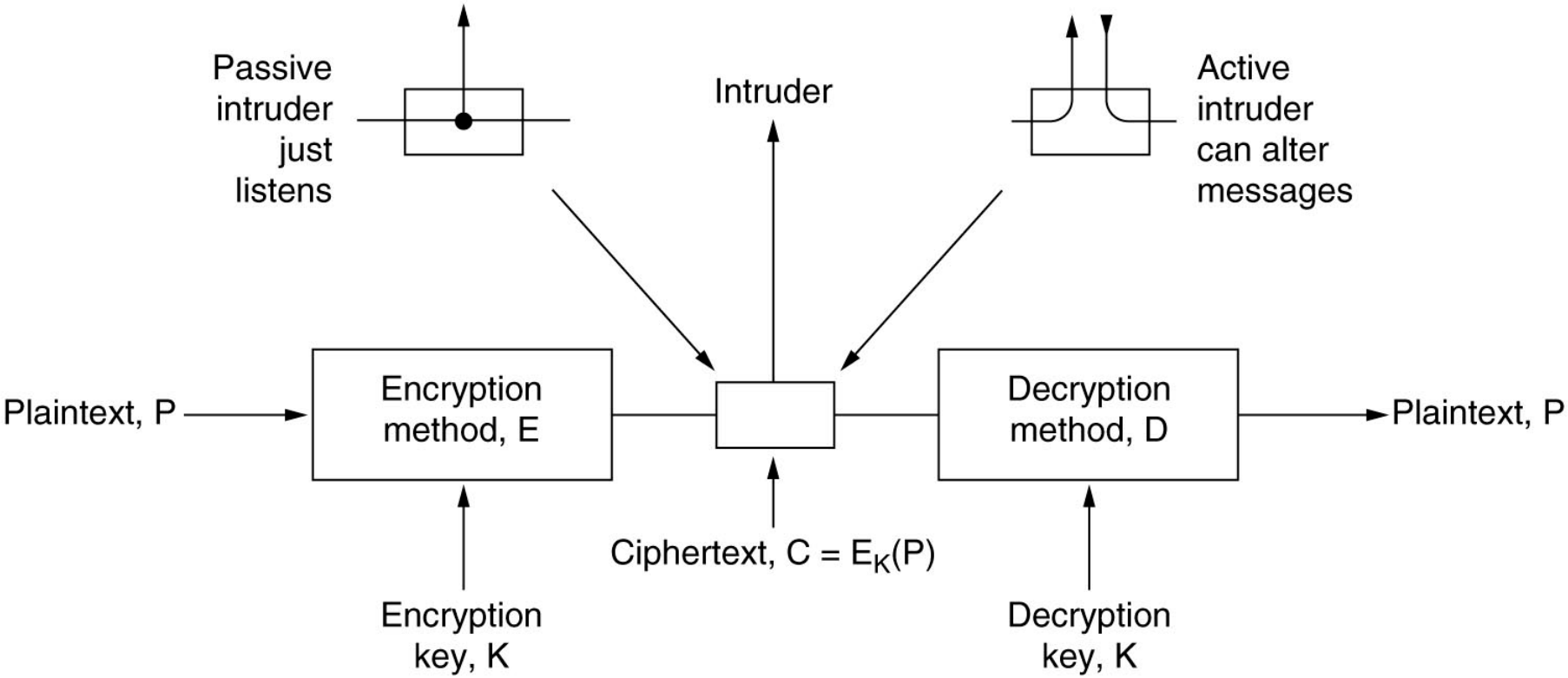
Security issues: some practical situations

- A sends a file to B: E intercepts it and reads it
  - How to send a file that looks gibberish to all but the intended receiver?
- A send a file to B: E intercepts it, modifies it, and then forwards it to B
  - How to make sure that the document has been received in exactly the form it has been sent
- E sends a file to B pretending it is from A
  - How to make sure your communication partner is really who (s)he claims to be
- A sends a message to B: E is able to delay the message for a while
  - How to detect old messages
- A sends a message to B. Later A (or B) denies having sent (received) the message
  - How to deal with electronic contracts
- E learns which user accesses which information although the information itself remains secure
- E prevents communication between A and B: B will reject any message from A because they look unauthentic

Classes of network security problems

- **Secrecy (or confidentiality)**
  - Keep the information out of the hands of unauthorized users, even if it has to travel over insecure links
- **Authentication**
  - Determine whom you are talking to before revealing sensitive information
- **Non-repudiation (or signatures)**
  - Prove that the order was to buy X litres of alcohol at the price *before* the taxes fell down and not the price *after.* Prove also that the order indeed existed
- **Data integrity (or message authentication)**
  - Make sure that the message received was exactly the message you sent (not necessarily interested here in the confidentiality of the document)

Basic situation in cryptography



Basic situation in cryptography

- A(lice) sends a message (or file) to B(ob) through an open channel (say, Internet), where E(vil, nemy) tries to read or change the message
- A will **encrypt** the **plaintext** using a **key** transforming it into a "unreadable" **cryptotext**
  - This operation must be computationally easy
- B also has a key (say, the same key) and **decrypts** the cryptotext to get the plaintext
  - This operation must be computationally easy
- E tries to **cryptanalyze**: deduce the plaintext (and the key) knowing only the cryptotext
  - This operation should be computationally difficult
- We will use **cryptography** to cover both the design of secure systems and their **cryptanalysis** – **cryptology** is also used sometimes
  - *Do not think in terms of good guys do cryptography and bad guys do cryptanalysis*

Cryptography – some types of systems

- Depending on the type of operations in the encryption/decryption
  - Based on substitutions: elements in the plaintext are replaced by other elements
  - Based on transpositions: elements in the plaintext are re-arranged
- Number of keys used
  - Symmetric systems (also known as single-key, secret-key, or conventional systems)
  - Asymmetric systems (also known as two-key, public-key, or unconventional systems)
- The way the plaintext is processed
  - Block ciphers: plaintext split into blocks processed separately
  - Stream ciphers: plaintext processed continuously

Cryptanalysis – types of attacks

- **Fundamental rule**: one must always assume that the attacker knows the methods for encryption and decryption; he is only looking for the keys
  - Creating a new cryptographic method is a very complex process involving many people – difficult to keep it confidential
  - Bonus for publishing the methods: people will try to break it for you (for free!)
- **Passive attack**: the attacker only monitors the traffic attacking the confidentiality of the data
- **Active attack**: the adversary attempts to alter the transmission attacking data integrity, confidentiality, and authentication.

- **Cryptanalysis**: rely on the details of the encryption algorithm plus perhaps some knowledge about the general characteristics of the plaintext – sometimes the plaintext is known and the *key* is being looked for
- **Brute-force attack**: try every possible key on the ciphertext until an intelligible translation into a plaintext is obtained

Key Size (bits)	Number of Alternative Keys	Time required at 1 decryption/μs	Time required at 10^6 decryptions/μs
32	$2^{32} = 4.3 \times 10^9$	2^{31} μs = 35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	2^{55} μs = 1142 years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	2^{127} μs = 5.4×10^{24} years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	2^{167} μs = 5.9×10^{36} years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	2×10^{26} μs = 6.4×10^{12} years	6.4×10^6 years

Source: W.Stallings Cryptography and network security, 5th edition, 2011 (Table 2.2).

Attacks on encryption schemes

Type of attack	Known to cryptanalyst
Ciphertext only	■ *Encryption algorithm* ■ *Ciphertext*
Known plaintext	■ *Encryption algorithm* ■ *One or more pairs plaintext-ciphertext*
Chosen plaintext	■ *Encryption algorithm* ■ *One or more pairs plaintext-ciphertext, with the plaintext chosen by the attacker*
Chosen ciphertext	■ *Encryption algorithm* ■ *Several pairs plaintext-ciphertext, ciphertext chosen by the attacker*

Attacks on protocols

- **Known-key attack**: obtain some previous keys and use the information to get the new ones
- **Replay**: the adversary records a communication session and replays the entire session or portions of it at a later time
- **Impersonation**: adversary assume the identity of a legitimate user
- **Dictionary**: the attacker has a list of probable passwords, hashes them and compares with the entries in the list of true encrypted passwords hoping to get a match

How secure is secure?

- **Evaluating the security of a system is a crucial and most difficult task**
- **Unconditionally secure system**
  - If the ciphertext does not contain enough information to determine uniquely the corresponding ciphertext: any plaintext may be mapped into that ciphertext with a suitable key
  - Consequently, the attacker cannot find the plaintext regardless of how much time and computational power he has because the information is not there!
  - **Bad news:** only one known system has this property: **one-time pad**
- **Complexity-theoretic security**
  - Consider a model of computation (e.g., Turing machine) and adversaries modeled as having polynomial computational power
  - Consider the weakest possible assumptions and the strongest possible attacker and do worst-case or at least average-case analysis

How secure is secure?

- **Provable security**
  - Prove that breaking the system is equivalent with solving a *supposedly* difficult (math) problem (e.g., from Number Theory)
- **Computationally secure**
  - The (perceived) cost of breaking the system exceeds the value of the encrypted information
  - The (perceived) time required to break the system exceeds the useful lifetime of the information

How large is large?

Reference	Order of magnitude
Seconds in a year	$\approx 3 \times 10^7$
Age of our solar system (years)	$\approx 6 \times 10^9$
Seconds since creation of solar system	$\approx 2 \times 10^{17}$
Clock cycles per year, 3 GHz computer	$\approx 9.6 \times 10^{16}$
Binary strings of length 64	$2^{64} \approx 1.8 \times 10^{19}$
Binary strings of length 128	$2^{128} \approx 3.4 \times 10^{38}$
Binary strings of length 256	$2^{256} \approx 1.2 \times 10^{77}$
Number of 75-digit prime numbers	$\approx 5.2 \times 10^{72}$
Electrons in the universe	$\approx 8.37 \times 10^{77}$

Adapted from Handbook of Applied Cryptography (A.Menezes, P.van Oorschot, S.Vanstone), 1996

Overview of the course

- I. CRYPTOGRAPHY
  - Secret-key cryptography
    - Classical encryption techniques
    - DES, AES, RC5, RC4
  - Public-key cryptography
    - RSA
  - Key management
- II. AUTHENTICATION
  - MAC
  - Hashes and message digests
  - Digital signatures
  - Kerberos
- III. NETWORK SECURITY
  - Email security
  - IP security
  - Web security (SSL, secure electronic transactions)
  - Firewalls
  - Wireless security
- IV. OTHER ISSUES
  - Viruses
  - Digital cash
  - Secret sharing schemes
  - Zero-knowledge techniques

About the course

- The goal of this course is to present the basic ideas and concepts of cryptography and network security
- Huge amount of interesting/useful/challenging issues skipped
- This should be thought of as an “Introduction to…” course
- We will go occasionally into considerations of more advanced math (finite fields, modular arithmetic, number theory)
  - No surprise here: the whole idea of cryptography is centered around difficult problems that cannot be solved unless a trap-door (key) is known
  - No assumptions made on the math background – all notions will be introduced whenever needed
  - No need to be taken aback by the math part

Administrative details

- Webpage: http://users.abo.fi/ipetre/crypto/
- Email address: ion.petre@abo.fi
- Exam: 30 points for maximum mark, 15 to pass
  - Not necessarily interested in the full details of the algorithms/protocols
  - Rather on the structure of an algorithm/protocol, the rationale behind that structure
  - Breaking or designing simple systems (simple enough for paper and pencil only)
  - Ideas, notions, etc.
- Course book: W. Stallings – “Cryptography and network security”
- Other useful books:
  - C.Kaufman, R.Perlamn, M.Speciner – “Network security. Private communication in a public world”
  - W.Trappe, L.Washington – “Introduction to cryptography with coding theory”
  - See the course website for more suggested reading

Challenges

- No exercises
  - Optional assignments offering a number of points
  - If one collects sufficiently many points, (s)he may skip exam
  - *Protocol*
    - *announce the challenge at the end of a lecture*
    - *allow for a couple of days before the data is published on the course website*
    - *award the points to the first N correct answers received in the lecturer's inbox (email only!) before a deadline*