Ceng 471 - Cryptography

Asst. Prof. Dr. Serap Şahin
Izmir Institute of Technology
Department of Computer Engineering

Outline

- What is the Cryptography?
- A Brief History
- Cryptographic Goals and Evaluation Criteria for Cryptographic Tools
- Basic Terminology and Concepts

- What is the Cryptography for your daily life?

What is the Cryptography?

- Computer security is an important field of study for most day-to-day transactions.
  - Our cellular phones, check our voice mail and e-mail, use debitor credit cards, order a pay-per view movie, use a transponder through EZ-Pass, login to social services, sign on to online video games, and even during visits to the doctor.
  - It is also often used to establish virtual private networks (VPNs) and Secure Shell connections (SSH), which allows employees to telecommute and access computers remotely.

What is the Cryptography?

- Cryptography is the automated (or algorithmic) method in which security goals are accomplished.
- Typically, when we say "crypto algorithm" we are discussing an algorithm meant to be executed on a computer. These algorithms operate on messages in the form of groups of bits.
- It is perhaps most popular, as it is the oldest cryptography related security goal and feeds into our natural desire to have secrets. Secrets in the form of desires, wants, faults, and fears are natural emotions and thoughts all people have. It of course helps that modern Hollywood plays into this with movies such as Swordfish and Mercury Rising.

What is the Cryptography?

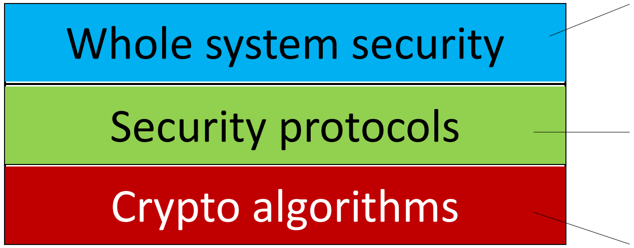
- Definition of Cryptography
  - *Cryptography is the study of mathematical techniques related to aspects of information* security such as confidentiality, data integrity, entity authentication, and data origin authentication.
  - Cryptography is about the prevention and detection of cheating and other malicious activities.

Information Security

InfoSec:

- Computer Security: deals mostly with access control
- Network Security: deals with communications security

Layers of a Security System:



Whole system security

Security protocols

Crypto algorithms

includes everything: policy management, administration, personnel training, etc.

how to achieve a certain functionality using the crypto algorithms

fundamental building blocks

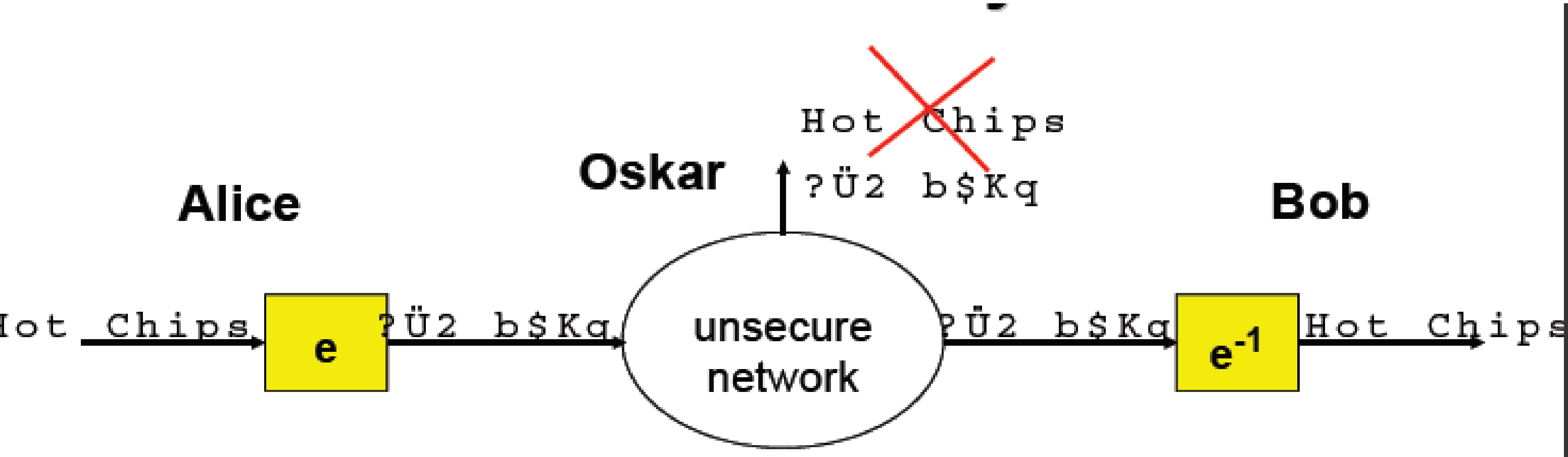
Main Issues

- confidentiality, privacy, secrecy
- authentication
- data integrity
- anonymity
- non-repudiation
- availability
- traceability

Cryptographic Goals

- Confidentiality is a service used to keep the content of information from all but those authorized to have it. Secrecy is a term synonymous with confidentiality and privacy.
  - There are numerous approaches to providing confidentiality, ranging from physical protection to mathematical algorithms which render data unintelligible.

Confidentiality

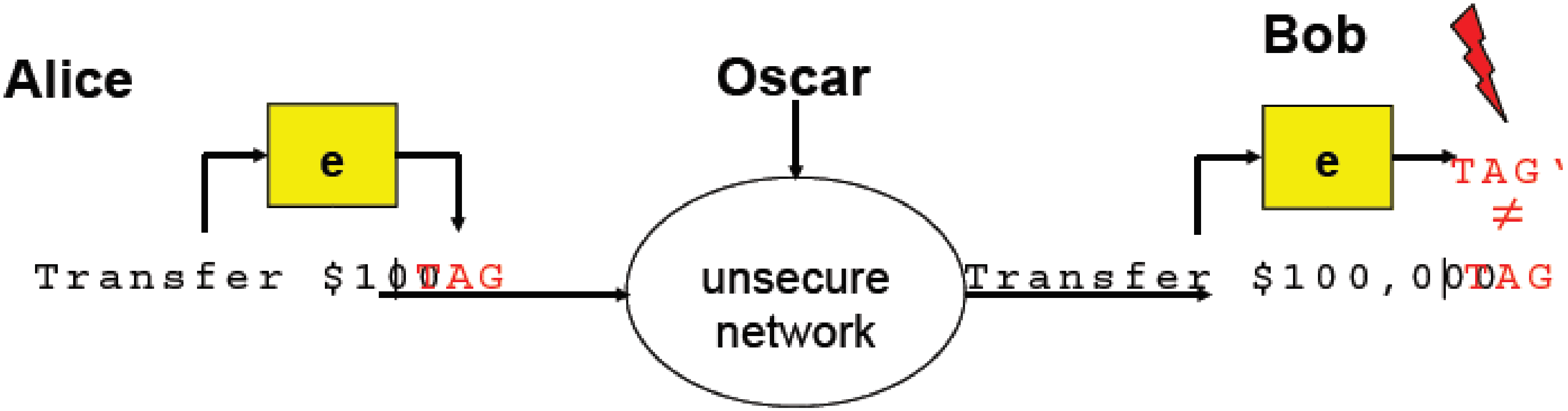


Encryption ensures **confidentiality** of messages

Cryptographic Goals

- Data integrity is a service which addresses the unauthorized alteration of data.
  - To assure data integrity, one must have the ability to detect data manipulation by unauthorized parties.
  - Data manipulation includes such things as insertion, deletion, and substitution.

Integrity of Messages



Cryptographic authentication tags:

2. Message Authentication Codes (MAC), or
3. digital signatures

ensure the **integrity** of messages

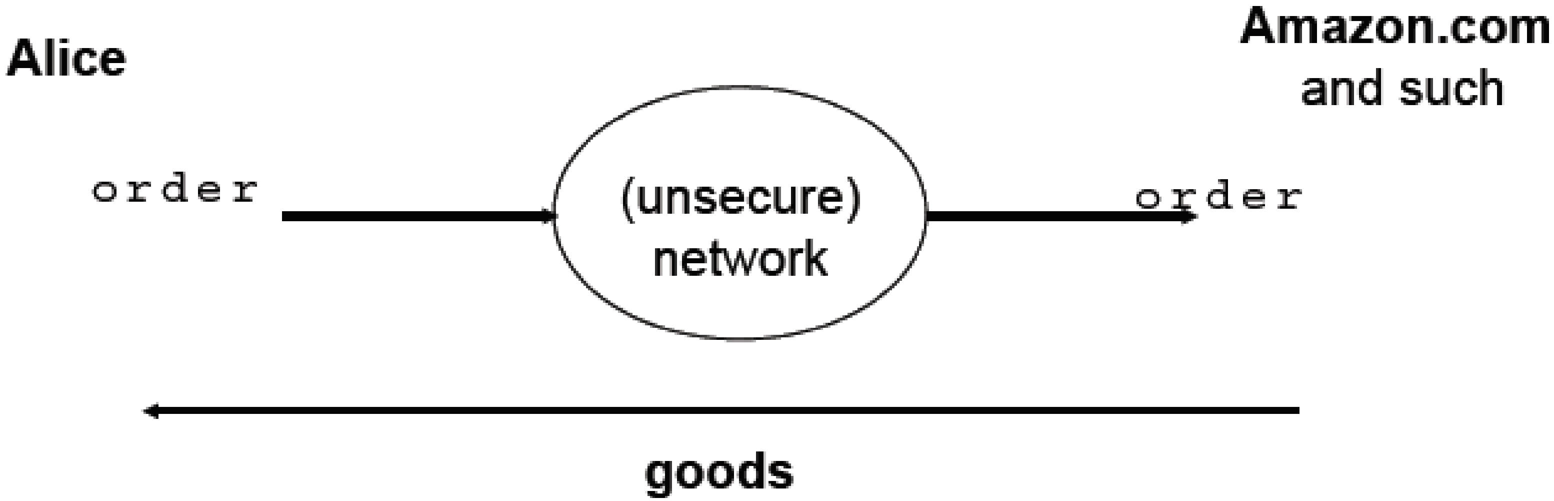
Cryptographic Goals

- Authentication is a service related to identification.
  - Two parties entering into a communication should identify each other.
  - Information delivered over a channel should be authenticated as to origin, date of origin, data content, time sent, etc.

Cryptographic Goals

- Non-repudiation *is a service which prevents an entity from denying previous commitments* or actions.
  - When disputes arise due to an entity denying that certain actions were taken, a means to resolve the situation is necessary.
    - For example, one entity may authorize the purchase of property by another entity and later deny such authorization was granted. A procedure involving a trusted third party is needed to resolve the dispute.

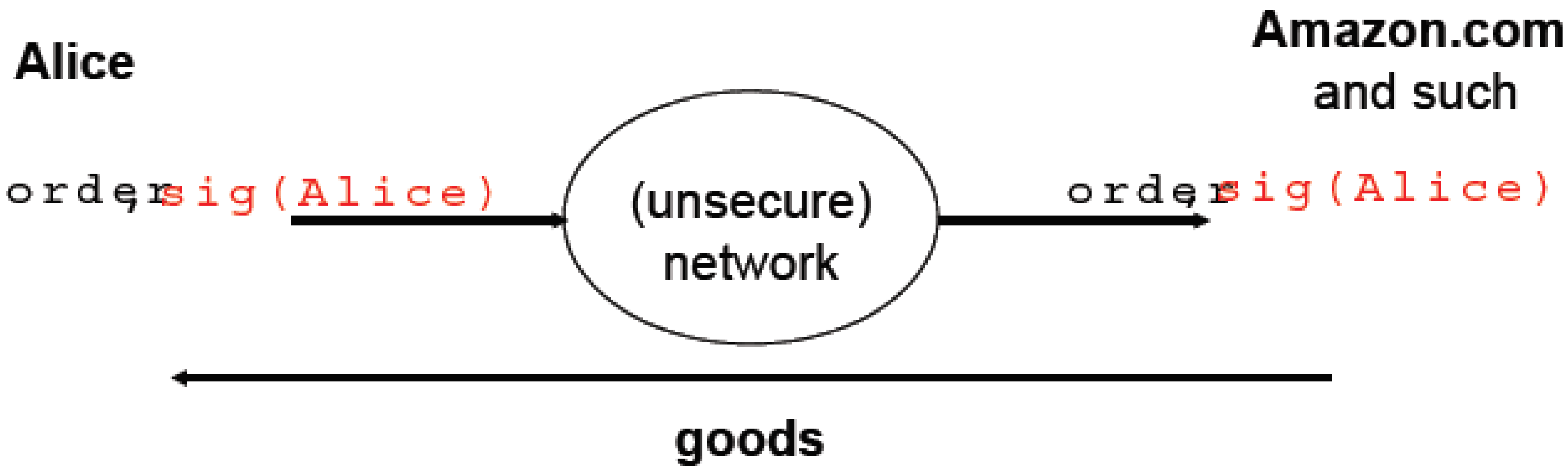
Non-Repudiation: Why we need it?



without non-repudiation:

2. Alice orders at favorite eCommerce vendor
3. stuff gets delivered
4. Alice doesn‘t feel like buying: „I never ordered this“
5. vendor can not **proof** it (big monetary issue if vendor = BMW.com)

Non-Repudiation: How it works?



Alice

Amazon.com
and such

order sig(Alice)

(unsecure)
network

order sig(Alice)

goods

with non-repudiation:

2. Alice orders at favorite eCommerce vendor
3. stuff gets delivered
4. Alice doesn‘t feel like buying: „I never ordered this“
5. vendor sues Alice: **proof** of order through Alice‘s signature

Non-repudiation is strong point of digital signatures

Basic Terminology and Concepts

Encryption domains and codomains

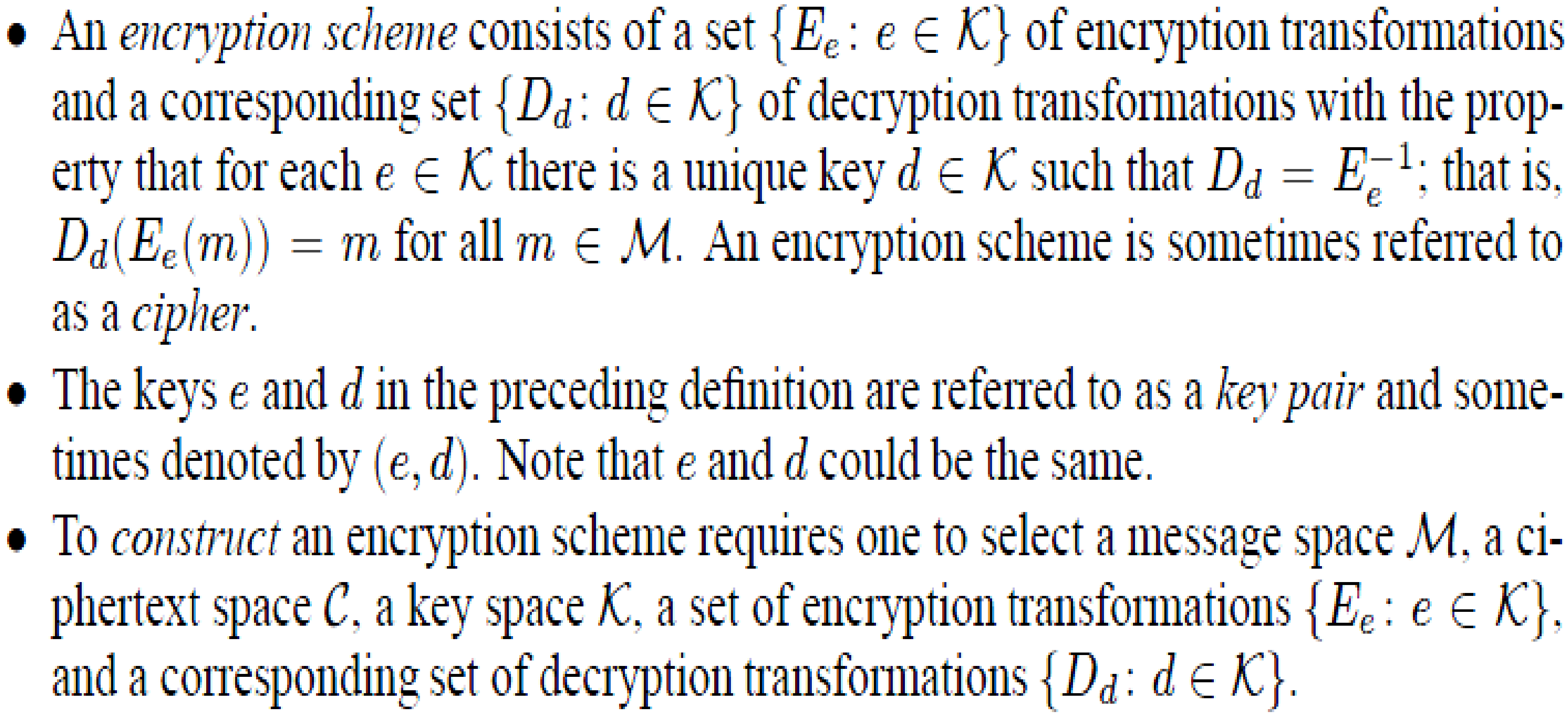
- “A” denotes a finite set called the *alphabet of definition. For example, A = {0; 1}, the binary alphabet, is a frequently used alphabet of definition. Note that any alphabet* can be encoded in terms of the binary alphabet.
- “M” denotes a set called the *message space. M consists of strings of symbols from* an alphabet of definition. An element of M is called a *plaintext message or simply* a *plaintext. For example, M may consist of binary strings, English text, computer* code, etc.
- “C” denotes a set called the *ciphertext space. C consists of strings of symbols from an* alphabet of definition, which may differ from the alphabet of definition for M. An element of C is called a *ciphertext.*

Basic Terminology and Concepts

Encryption and decryption transformations

- K denotes a set called the *key space*. *An element of K is called a key.*
- Each element e Є K uniquely determines a bijection from M to C, denoted by E_e.
- E_e is called an *encryption function or an encryption transformation.* *Note that* E_e must be a bijection if the process is to be reversed and a unique plaintext message recovered for each distinct ciphertext.
- For each d Є K, D_d denotes a bijection from C to M (i.e., $D_d : C \rightarrow M$). D_d is called a *decryption function or decryption transformation.*
- The process of applying the transformation E_e to a message m Є M is usually referred to as *encrypting m or the encryption of m.*
- The process of applying the transformation D_d to a ciphertext c is usually referred to as *decrypting c or the decryption of c.*

Basic Terminology and Concepts



- An *encryption scheme* consists of a set $\{E_e : e \in \mathcal{K}\}$ of encryption transformations and a corresponding set $\{D_d : d \in \mathcal{K}\}$ of decryption transformations with the property that for each $e \in \mathcal{K}$ there is a unique key $d \in \mathcal{K}$ such that $D_d = E_e^{-1}$; that is, $D_d(E_e(m)) = m$ for all $m \in \mathcal{M}$. An encryption scheme is sometimes referred to as a *cipher*.
- The keys e and d in the preceding definition are referred to as a *key pair* and sometimes denoted by (e, d). Note that e and d could be the same.
- To *construct* an encryption scheme requires one to select a message space $\mathcal{M}$, a ciphertext space $\mathcal{C}$, a key space $\mathcal{K}$, a set of encryption transformations $\{E_e : e \in \mathcal{K}\}$, and a corresponding set of decryption transformations $\{D_d : d \in \mathcal{K}\}$.

Basic Terminology and Concepts

Example (*encryption scheme*) Let $\mathcal{M} = \{m_1, m_2, m_3\}$ and $\mathcal{C} = \{c_1, c_2, c_3\}$. There are precisely $3! = 6$ bijections from $\mathcal{M}$ to $\mathcal{C}$. The key space $\mathcal{K} = \{1, 2, 3, 4, 5, 6\}$ has six elements in it, each specifying one of the transformations. Figure 1.5 illustrates the six encryption functions which are denoted by E_i, $1 \leq i \leq 6$. Alice and Bob agree on a transformation, say E_1. To encrypt the message m_1, Alice computes $E_1(m_1) = c_3$ and sends c_3 to Bob. Bob decrypts c_3 by reversing the arrows on the diagram for E_1 and observing that c_3 points to m_1.

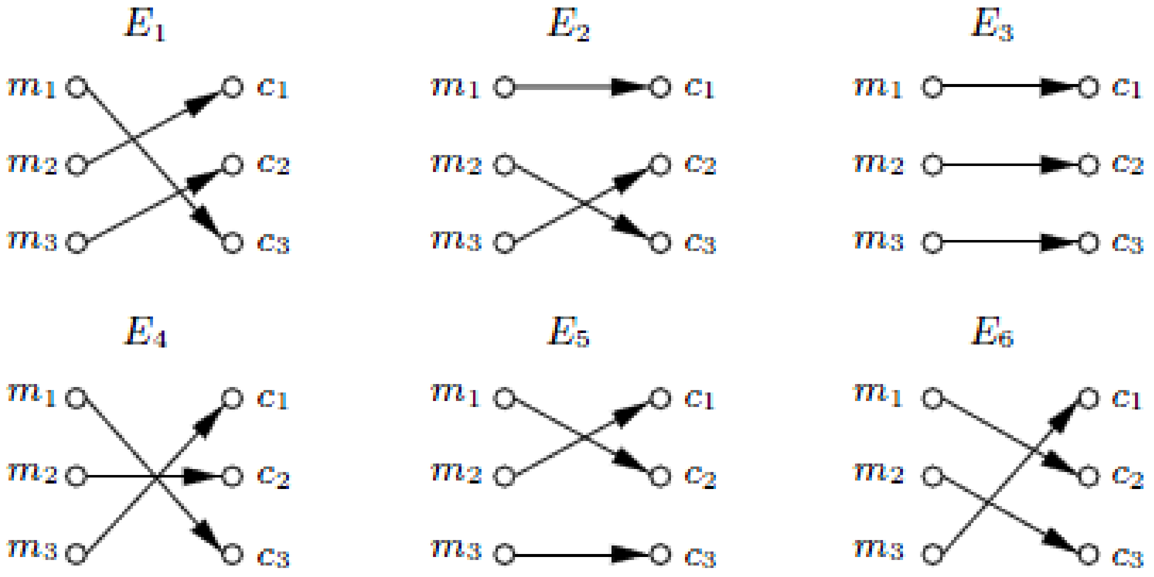


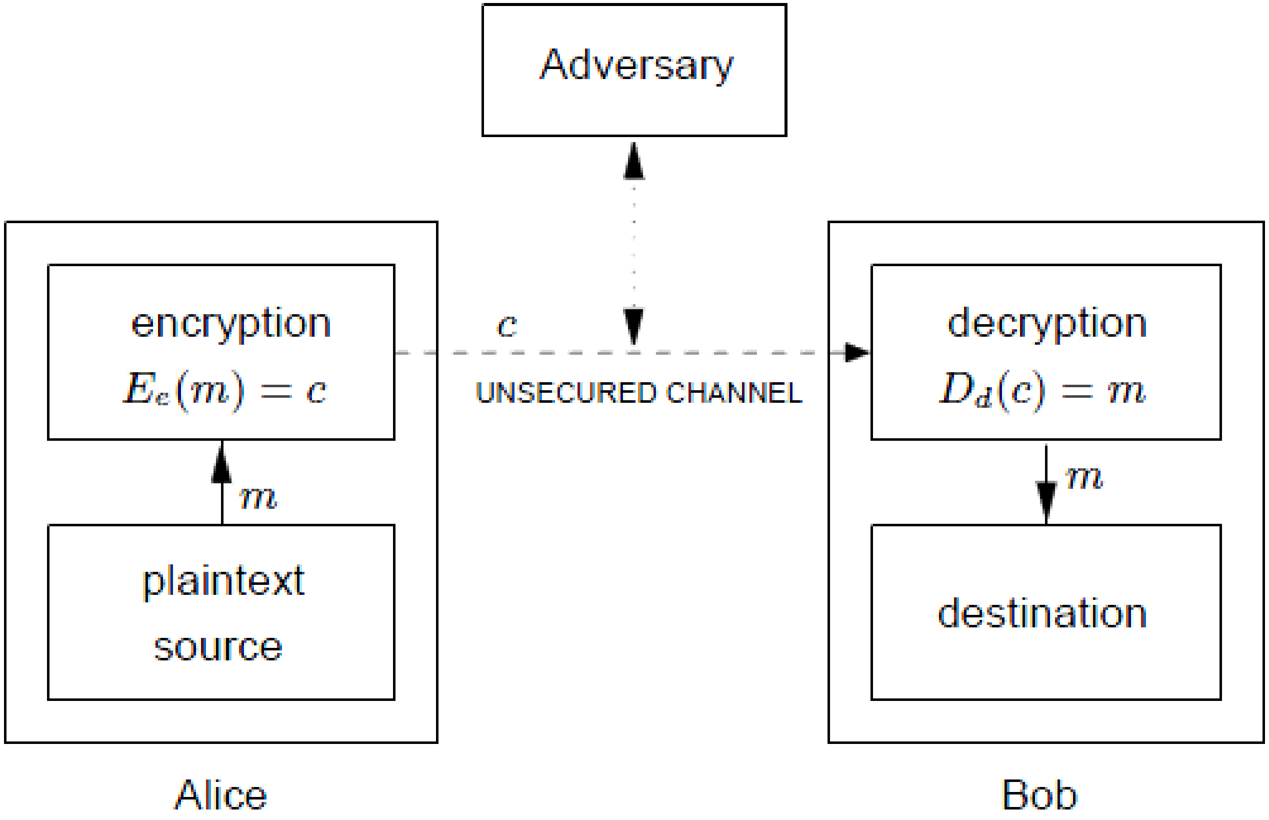
Figure 1.5: *Schematic of a simple encryption scheme.*

Basic Terminology and Concepts

- In cryptography, the set M is typically of astronomical proportions and, in these cases, new mathematical algorithms should use to describe the encryption and decryption transformations.

Basic Terminology and Concepts

- *Schematic of a two-party communication using encryption.*



Basic Terminology and Concepts

Communication participants

- An *entity* or *party is someone or something which sends, receives, or manipulates* information. Alice and Bob are entities. An entity may be a person, a computer terminal, etc.
- A *sender is an entity in a two-party communication which is the legitimate transmitter* of information. In figure, the sender is Alice.
- A *receiver is an entity in a two-party communication which is the intended recipient* of information. In Figure, the receiver is Bob.
- An *adversary is an entity in a two-party communication which is neither the sender* nor receiver. Various other names are synonymous with adversary such as enemy, attacker, opponent, tapper, eavesdropper, intruder, and interloper.
  - An adversary will often attempt to play the role of either the legitimate sender or the legitimate receiver.

Basic Terminology and Concepts

Channels

- A *channel is a means of conveying information from one entity to another.*
- A *physically secure channel or secure channel is one which is not physically accessible* to the adversary.
- An *unsecured channel is one from which parties other than those for which the information* is intended can reorder, delete, insert, or read.
- A *secured channel is one from which an adversary does not have the ability to reorder,* delete, insert, or read.

Basic Terminology and Concepts

- An *information security service is a method to provide some specific aspect of security.*
  - For example, integrity of transmitted data is a security objective, and a method to ensure this aspect is an information security service.
- *Breaking an information security service (which often involves more than simply encryption)* implies defeating the objective of the intended service.
- A *passive adversary is an adversary who is capable only of reading information from* an unsecured channel.
- An *active adversary is an adversary who may also transmit, alter, or delete information* on an unsecured channel.

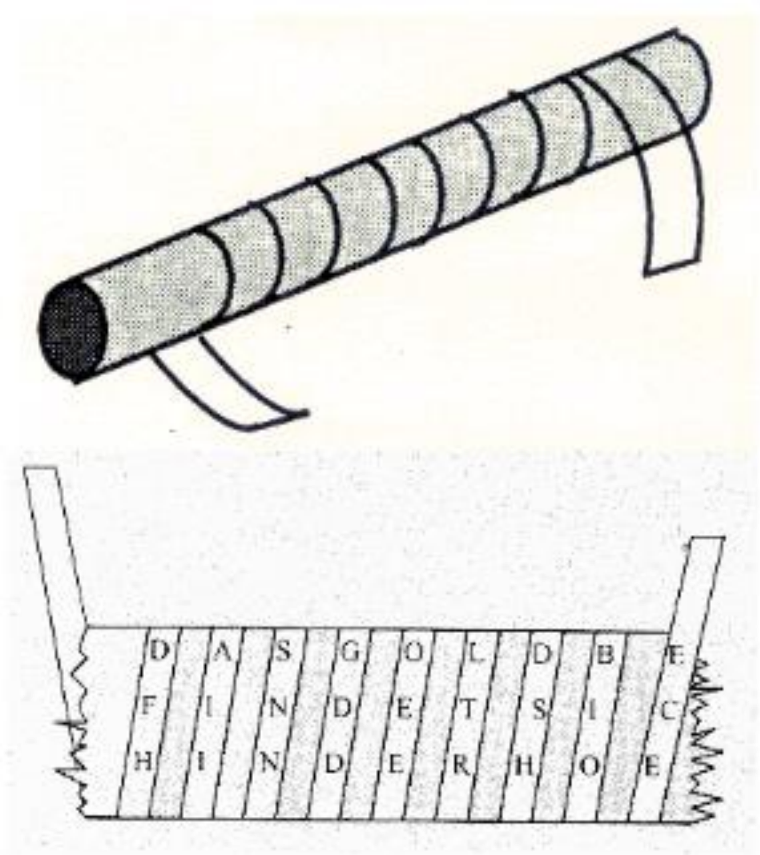
Basic Terminology and Concepts

Cryptology

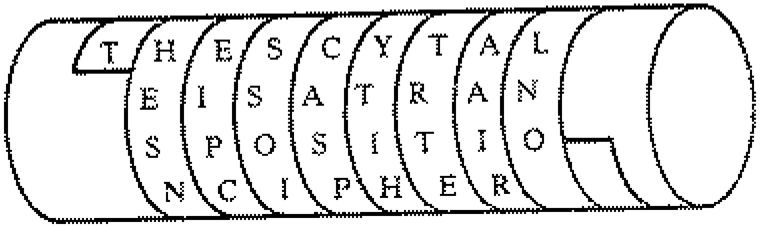
- Cryptanalysis is the study of mathematical techniques for attempting to defeat cryptographic techniques, and, more generally, information security services.
- A cryptanalyst is someone who engages in cryptanalysis.
- Cryptology is the study of cryptography and cryptanalysis.
- A cryptosystem is a general term referring to a set of cryptographic tools used to **provide information security services**. Most often the term is used in conjunction with primitives providing confidentiality, i.e., encryption.

A Brief History for Cryptography

Cryptography, ca. 500 B.C



Skytale of Sparta



THE SCYTALE IS A TRANSPOSITION CIPHER

A Brief History for Cryptography

- **Old cryptography** methods relied on elementary operations on the symbols of the initial text, a simple example being to replace each letter by another one following a given rule which was supposed to be known only by the sender and the receiver. (Julius Caesar)
- it is easy to decipher such messages without knowing the key, and one can even recover the key from an encoded message.
- To break such a code, one efficient process is to perform a statistical study of occurrences of the different letters. This idea was used as early as IX th. century by Abu Youssouf Yaqub Ishaq Al Kindi.

Some Historical Examples

- **Shift Cipher:**
  - For an n-letter alphabet,
    $P,C,K \in Z_n$
    $E_K(P) = P + K \bmod n$
    $D_K(C) = C - K \bmod n$.
  - Cryptanalysis: exhaustive key search
- **Substitution Cipher:**
  - $P,C \in Z_n$; K is a bijection, f, over Z_n
    $E_K(P) = f(P)$
    $D_K(C) = f^{-1}(C)$.
  - Cryptanalysis: frequency analysis

A Brief History for Cryptography

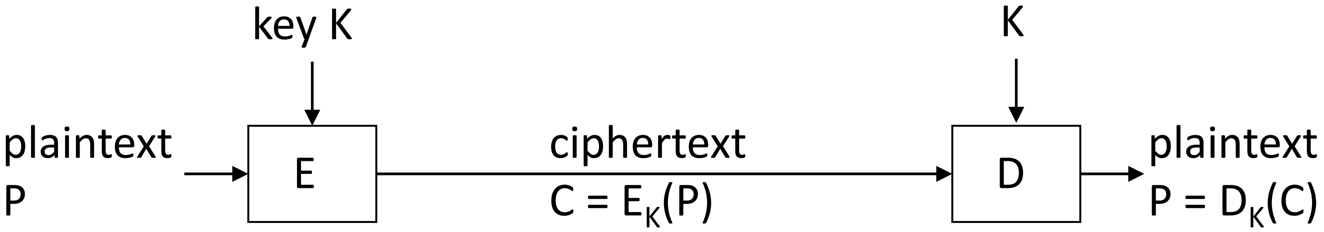
- During the XIII-th century, in his Letter concerning the Marvelous Power of Art and Nature and the Nullity of Magic, Roger Bacon described seven methods to encrypt messages in 1200s.
- In the XVI-th century, the French diplomat Blaisede Vigenere was also a cryptographer. He invented Vigenere cyphering.
- C. Babbage (1791-1871), who invented the computer, pointed out the usefulness of statistics for deciphering encrypted messages.
- After the war in 1870 between France and Germany, the French Government realized that one strong point of the German army was communication; it was decided to create military centers for the study of carrier-pigeons.
- At the same time, James C. Maxwell was developing electromagnetism theory, and H. H. Herz and Acharya J. C. Bose, was going to give rise to radio and modern means of transmitting data.

A Brief History for Cryptography

- In a visionary paper on the military cryptography published in the Journal of Military Sciences in 1883, A. Kerckhoffs proposed a number of principles which are still valid .
  - Such as; the security of the system must rely only on the choice of the keys, which should be renewed on a regular basis.

Cryptographic Fundamentals

- Basic encryption:



Key: An easy-to-change, variable parameter of the encryption algorithm.

- Kerckhoffs' principle (1883):
  Security should not rely on the secrecy of the algorithm; everything may be known but the key.

A Brief History for Cryptography

- The red phone (which was a fax) between White House and Kremlin during the cold war used the disposable mask technique which had been invented by G. Vernam in 1917.
- During World War II (1940), most German communications were enciphered on the Enigma cipher machine. It was comprised a series of rotor wheels with internal cross-connections, providing a substitution using a continuously changing alphabet.

Some Historical Examples

- Vernam Cipher (1917):
  - $P, C, K \in \{0,1\}^n$, for some $n \geq 1$.
    $E_K(P) = P \oplus K$
    $D_K(C) = C \oplus K$
  - Problem: Key needs to be transmitted, which is as long as the message.
  - Used for top-secret applications (E.g., Washington-Moscow red line)

Vernam Cipher (cont.)

Perfect Secrecy (Shannon, 1949): Ciphertext leaks no information about the message.

Theorem: Vernam cipher has perfect secrecy if each key bit is generated uniformly randomly.

Theorem: For perfect secrecy, the entropy of the key has to be at least as high as the entropy of the message. (i.e. the key has to be at least as long as the message.)

A Brief History for Cryptography

- The mathematician A.Turing invented a code breaking machine, the Bomb, which gave birth to the first electronic programmable computer by Max Newman.
  - The work done by him and his colleagues at Bletchley Park brought cryptology in to the modern world .
- It required in genius logic, statistical theory, the beginnings of information theory, advanced technology, and superb organization.

A Brief History for Cryptography

- C. Shannon, an American electrical engineer and mathematician, has been called `the father of information theory':
  - He pioneered the modern mathematical theory of data transmission.
- The principles of using public keys for enciphering messages was suggested by W. Diffie and M. E. Hellman in 1976 ;
- Its first realization in 1978 by R. L. Rivest, A.Shamir and L.M.Adleman produced the RSA system which is now a days the most efficient.

Modern Ciphers

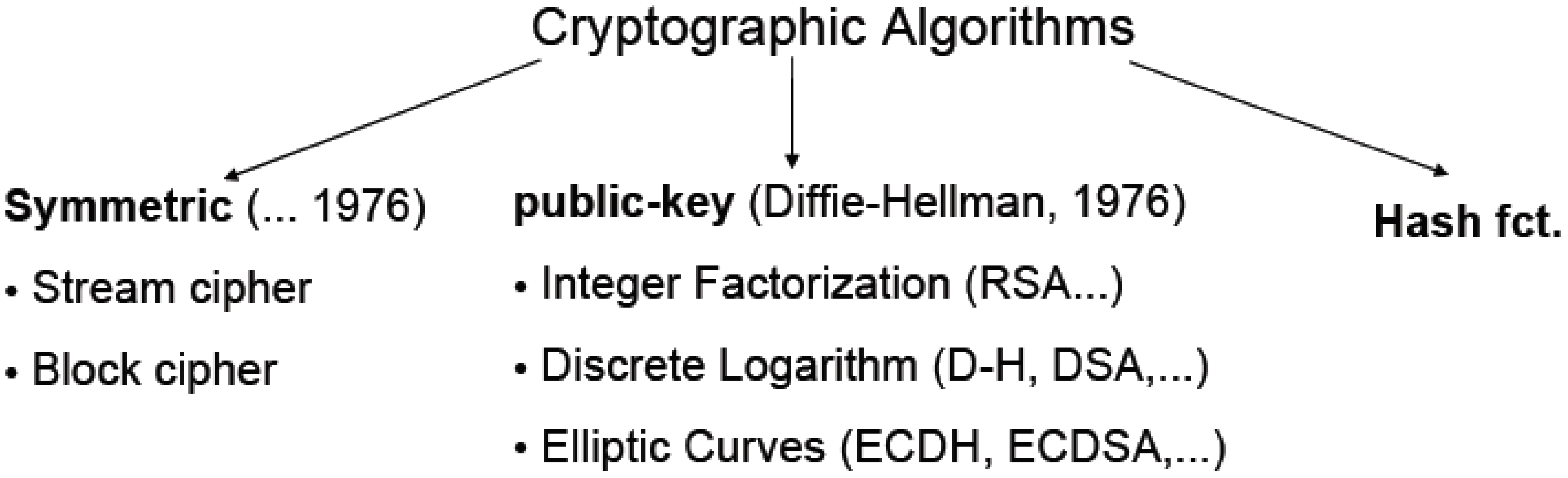
Shortcomings of historical systems:

- Substitution cipher: Small size of the input domain, which enables frequency analysis.
- Vernam cipher: Unlimited key size, which makes key generation and exchange a problem.

Modern ciphers:

- Block ciphers: Increasing the size of the input alphabet (i.e. blocks) for substitution
- Stream ciphers: Using a PRNG for generating the key stream

Cryptographic Toolkit



Cryptographic Algorithms

Symmetric (... 1976)

- Stream cipher
- Block cipher

public-key (Diffie-Hellman, 1976)

- Integer Factorization (RSA...)
- Discrete Logarithm (D-H, DSA,...)
- Elliptic Curves (ECDH, ECDSA,...)

Hash fct.

Cryptography, ca. 1990

Sparkasse Trier
CARD
GeldKarte
Diese Karte ist hinsichtlich ihrer
GeldKartenfunktion übertragbar.
Bei Verlust keine Erstattung des in
der GeldKarte enthaltenen Betrages.
Karten-Nr.
GeldKartenfunktion
gültig bis

Smart card for banking applications

Cryptography, ca. 2000

Electronic road toll

Cryptography:

- prevents cheating **by** drivers
- protects privacy **of** drivers

Cryptography, ca 2010

Brave new pervasive world

#2 Bridge sensors

#3 Cleaning robots

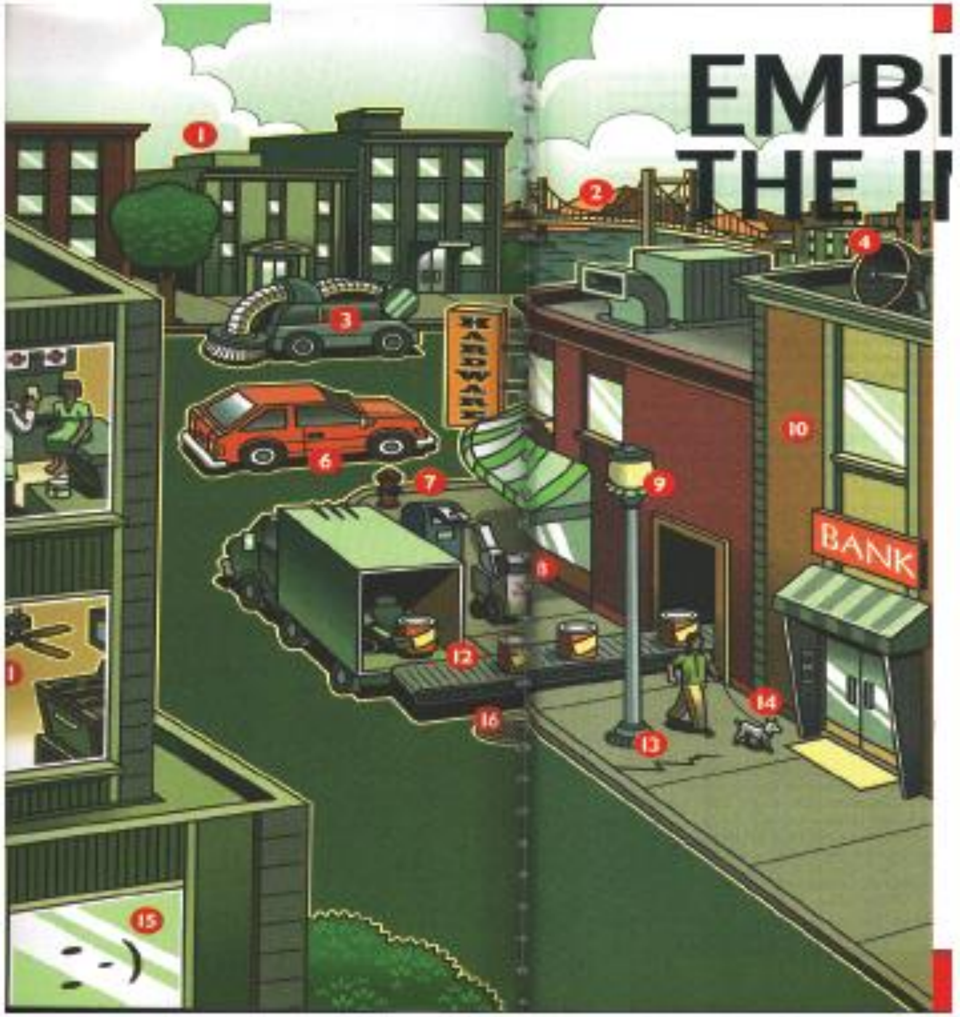
#6 Car with Internet access

#8 Networked robots

#9 Smart street lamps

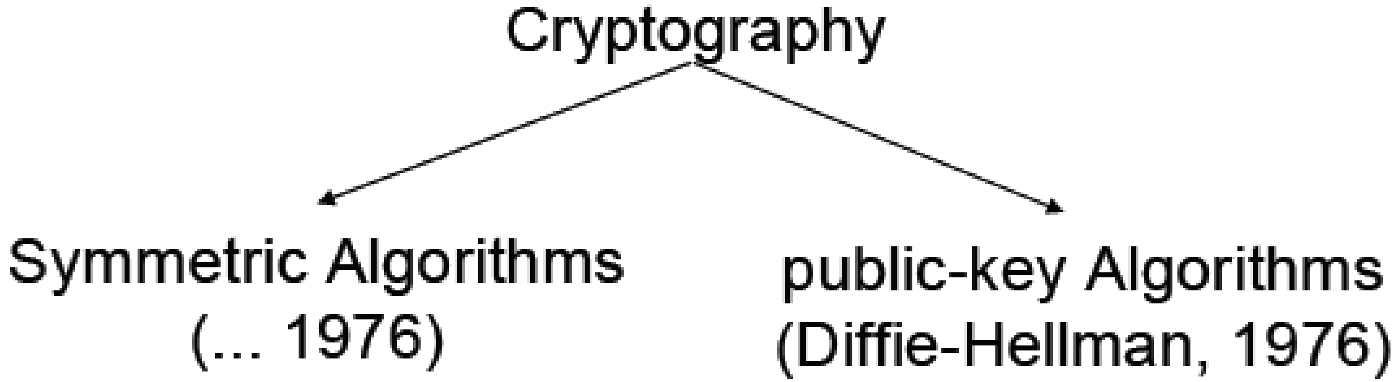
#14 Pets with electronic sensors

#15 Smart windows



IT Security and Cryptography

1. IT Security ≠ Cryptography
2. **but**: cryptography is an important **tool** for achieving IT security



Cryptography

Symmetric Algorithms
(... 1976)

public-key Algorithms
(Diffie-Hellman, 1976)

Evaluation Criteria for Cryptographic Tools

- Level of Security
- Functionality
- Methods of Operation
- Performance
- Easy of Implementation

The relative importance of various criteria is very much dependent on the application and resources available.

For example, in an environment where computing power is limited one may have to trade off a very high level of security for better performance of the system as a whole.

Evaluation Criteria for Cryptographic Tools: Level of Security

- This is usually difficult to quantify. Often it is given in terms of the number of operations required (using the best methods currently known) to defeat the intended objective.
  - Typically the level of security is defined by an upper bound on the amount of work necessary to defeat the objective.(Work Factor, W_d)

Evaluation Criteria for Cryptographic Tools: Functionality

- Tools will need to be combined to meet various information security objectives.
- Which tools are most effective for a given objective will be determined by the basic properties of the tools.

Evaluation Criteria for Cryptographic Tools: Methods of Operation

- Tools, when applied in various ways and with various inputs, will typically exhibit different characteristics;
  - thus, one tool could **provide very different functionality depending on its mode of operation or usage.**

Evaluation Criteria for Cryptographic Tools: Performance

- This refers to the efficiency of a tool in a particular mode of operation.
  - For example, an encryption algorithm may be rated by the number of bits per second which it can encrypt.

Evaluation Criteria for Cryptographic Tools: Easy of Implementation

- This refers to the difficulty of realizing the tool in a practical instantiation.
- This might include **the complexity of implementing the tool in either a software or hardware environment**.