Теория Информации

Ярмолик Вячеслав Николаевич

Лекция 1

2015

Contents

Introduction**:** Data security. Fundamental concepts of cryptography.

Transposition and Substitution ciphers**:** Simple transposition. Product cipher. Simple substitution cipher. Caesar cipher. Vigener cipher.

Mono and Poly alphabetic substitution cipher**:** Playfair cipher.

Rotor machines. The Enigma: a unique rotor machine.

***Data Encryption Standard* (DES):** History of the DES. DES algorithms.Weak and semi weak keys. Advanced DES versions. IDEA. Blowfish.

***Advanced Encryption Standard* (AES):** Reindgiil Algorithm.

Number theory**:** Prime numbers. Euler's function. Euler's theorem. Congruence.

Public Key Cipher**:** Principles of the public key cipher. One-way function. Deffie and Hellman algorithm.

Contents *cont.*

***RSA Cipher*: Riverst, Shamir and Adleman public key cipher. Practical aspects.**

***Linear Feedback Shift Register*: Pseudorandom key generation by LFSR. M- sequences.**

***Stream cipher*: Synchronous stream ciphers. Self-synchronizing cipher.**

***Cryptographic Keys Management*: Keys generation, distribution and athetifacation of Public Keys**

***Communication Security*: Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL).**

***Authentication Protocols*: Password- authentication key agreement protocols. Password Authentification Protocol (PAP)**

Contents *cont.*

Digital signature**:** Main definition. Digital signature based on Symmetric cryptosystem.

Hash Functions**:** Message authentication codes (MAC). MD5. SHA-1.

Digital Signature algorithms**:** RSA based digital signature. Digital Signature Standard (DSS). *ElGamal* signature scheme.

Digital Signature algorithms modifications: Blind signature. Group signature. Proxy signature.

Elliptic curve cryptography**:** Elliptic curve cryptosystem (ECC). Elliptic curve *Diffie-Hellman* algorithm. Elliptic curve *Menezes-Qu-Vanstone* cryptosystem.

Elliptic Curve Digital Signature Algorithm: ECDSA algorithm.

Quantum Cryptography**:** Quantum Key Distribution. BB84, B92, Entanglement-Based quantum fey distribution.

Contents *Cont.*

***Physical Cryptography*:** Physical unclonable function (PUF). Arbiter PUF. Ring oscillator PUF. SRAM based PUF.

***Steganography*:** Textual steganography. Graphical steganography. LSB, BPCS, ABCDE and PCT steganography.

***Watermarking and Fingerprinting*:** Patchwork method. Copyright Protection Watermarking for copy protection

***Software protection*:** Software watermarking, obfuscation, and tamper-proofing. Software dongle. Electronic keys.

***E-Commerce security*:** E-commerce security standards. SET protocol.

***Internet Banking security*:** Online Banking Security. Password and PIN security:

1. Романец, Ю.В. Защита информации в компьютерных системах и сетях / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин. – М.: Радио и связь, 1999. – 328 с.

2. Харин, Ю.С. Математические и компьютерные основы криптологии / Ю.С. Харин, В.И. Берник, Г.В. Матвеев, С.В. Агиевич. – Минск : Новое Знание, 2003. – 382 с.

3. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнаейр. – М. : ТРИУМФ, 2002. – 816 с.

4. Ярмолик, В.Н. Элементы теории информации. Практикум для студентов специальности “Программное обеспечение информационных технологий” / В.Н. Ярмолик, А.П. Занкович, С.С. Портянко. – Минск : БГУИР, 2007. – 40 с.

5. Ярмолик, В.Н. Криптография, стеганография и охрана авторского права / В.Н. Ярмолик, С.С. Портянко, С.В. Ярмолик. – Минск : Издательский центр БГУ, 2007. – с.

6. Грибунин, В.Г. Цифровая стеганография / В.Г. Грибунин, И. Н. Оков, И. В. Туринцев. – М. : СОЛОН-Пресс, 2002. – 272 с.

Introduction

Cryptography is the science and study of secret writing.

A ***cipher*** is a secret method of writing, whereby ***plaintext*** (or ***cleartext***) is transformed into ***ciphertext*** (***cryptogram***).

Encipherment (***encryption***) is the process of transforming plaintext into ciphertext.

Decipherment (***decryption***) is the reverse process of transforming ciphertext into plaintext. Both encipherment and decipherment are controlled by a cryptographic ***key*** or ***keys.***

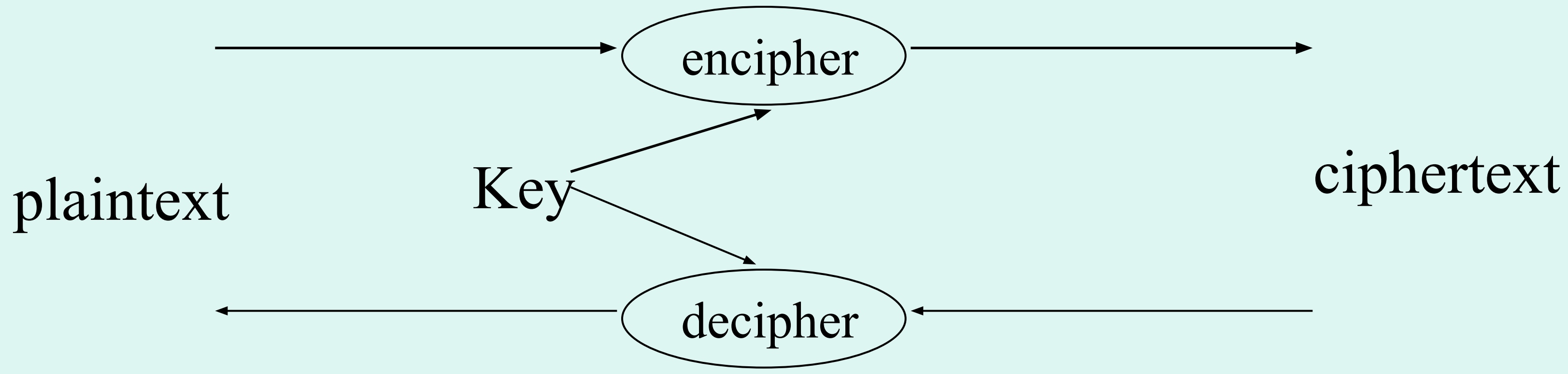

Fig.1.1. Secret writing

Introduction

Transposition ciphers

- There are two basic types of ciphers ***transpositions*** and ***substitutions.***
- ***Transposition ciphers*** rearrange bits or characters.
- The following simple example of the "*rail-fence*" cipher illustrate this method.

C	**R**	**Y**	**P**	**T**	**O**	**G**	**R**	**A**	**P**	**H**	**Y**
					⇓						
C				**T**				**A**			
	R		**P**		**O**		**R**		**P**		**Y**
		Y				**G**				**H**	
					⇓						
C	**T**	**A**	**R**	**P**	**O**	**R**	**P**	**Y**	**Y**	**G**	**H**

Fig.1.2. Rail-fence transposition cipher

Introduction

Substitutions ciphers

Substitution ciphers replace bits, characters, or blocks of characters with substitutes.

A simplest type of substitution cipher shifts each letter in the English alphabet forward by ***k*** positions cyclically (shifts past Z cycle back to A). ***k*** is the key to the cipher. This type of cipher is often called a *Caesar* cipher.

C R Y P T O G R A P H Y

$\Downarrow$

F U B S W R J U D S K B

Fig.1.3. Caesar's substitution cipher

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Introduction

Data Security

There are two principle objectives: ***secrecy*** (or ***privacy***), to prevent the unauthorized disclosure of data; and ***authenticity*** or ***integrity***), to prevent the unauthorized modification of data.

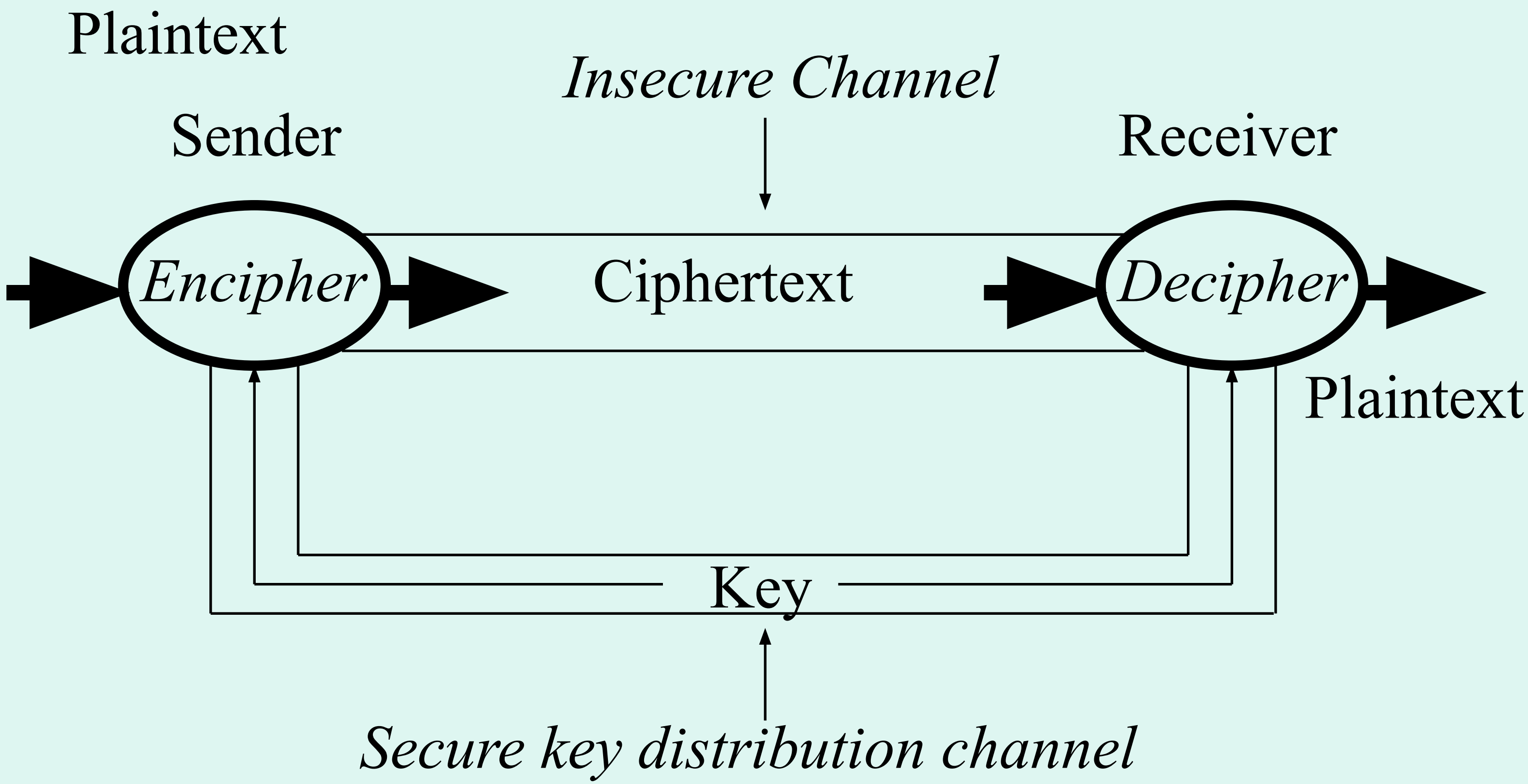

Fig.1.4. Classical information channel

Introduction
Cryptographic Systems

A ***cryptographic system*** (or ***cryptosystem*** for short) has five components:

1. A ***plaintext message space***, M.
2. A ***cipher message space***, C.
3. A ***key space***, k.
4. A family of ***enciphering transform.***, $Ek: M \dashrightarrow C$.
5. A family of ***deciphering transform.***, $Dk: C \dashrightarrow M$.

Cryptosystems General Requirements

1. The system must be easy to use.
2. The enciphering and deciphering transformations must be efficient for all keys.
3. The security of the system should depend only on the secrecy of the keys and not on the secrecy of the algorithms ***E*** and ***D***.

Introduction

Requirement for secrecy and authenticity

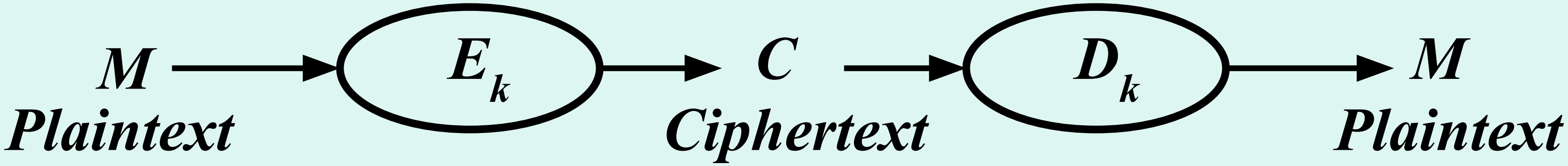

Fig.1.5. Cryptographic System.

Secrecy Requirements

1. It should be computationally infeasible for a cryptanalyst to systematically determine the deciphering transformation D_k from intercepted ciphertext C, even if the corresponding plaintext M is known.

2. It should be computationally infeasible for a cryptanalyst to systematically determine plaintext M from intercepted ciphertext C.

Authenticity Requirements

1. It should be computationally infeasible for a cryptanalyst to systematically determine the enciphering transformation E_k given C even if the corresponding plaintext M is known.

2. It should be computationally infeasible for a cryptanalyst to systematically find ciphertext C' such that $D_k(C')$ is valid plaintext in the set M.

Introduction

Simmons Cryptosystems Classifications

Simmons classifies cryptosystems as ***symmetric*** (***one-key***) and ***asymmetric*** (***two-key***).

In ***symmetric*** or ***one-key*** cryptosystems the enciphering and deciphering key are the same (or easily determined from each other). This means the transformations E_k and D_k are also easily derived from each other. Until recently, all cryptosystems were one-key systems only. There are also usually referred to as ***conventional*** (or ***classical***) systems.

One-key systems provide an excellent way of enciphering user's privite files. Each user A has private transformations E_k and D_k for enciphering and deciphering files.

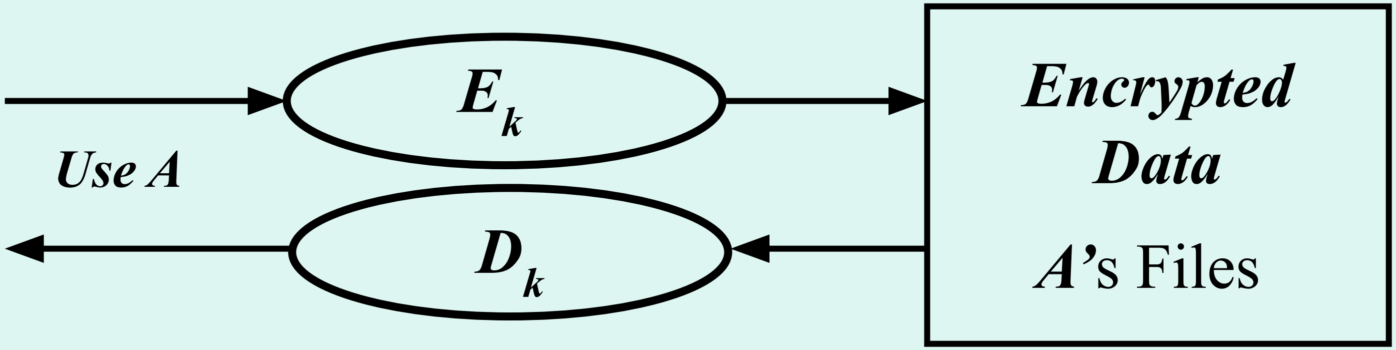

Fig.1.6. Single-key encryption of private files

Introduction

Public Key Cryptosystems

In a public-key system, each user *A* has a ***public transformation*** $\boldsymbol{E_A}$, which may be registered with a public directory, and a ***private transformation*** $\boldsymbol{D_A}$, which is known only to that user.

The private transformation $\boldsymbol{D_A}$ is described by a private key, and the public transformation $\boldsymbol{E_A}$ by a public key derived from the private key by one-way transformation. It must be computational infeasible to determine $\boldsymbol{D_A}$ from $\boldsymbol{E_A}$ (or even to fined a transformation equivalent to $\boldsymbol{D_A}$).

In a public-key system, secrecy and authenticity are provided by the separate transformations. Suppose user *A* wishes to send a message $\boldsymbol{M}$ to another user *B*. If *A* knows *B*'s public transformation $\boldsymbol{E_B}$, *A* can transmit $\boldsymbol{M}$ to *B* in secrecy by sending the ciphertext $C=\boldsymbol{E_B}(M)$. On receipt, *B* deciphers *C* using *B*'s private transformation , getting

$$\boldsymbol{D_B(C)=D_B(E_B(M))=M.}$$

Introduction

Public Key Cryptosystems

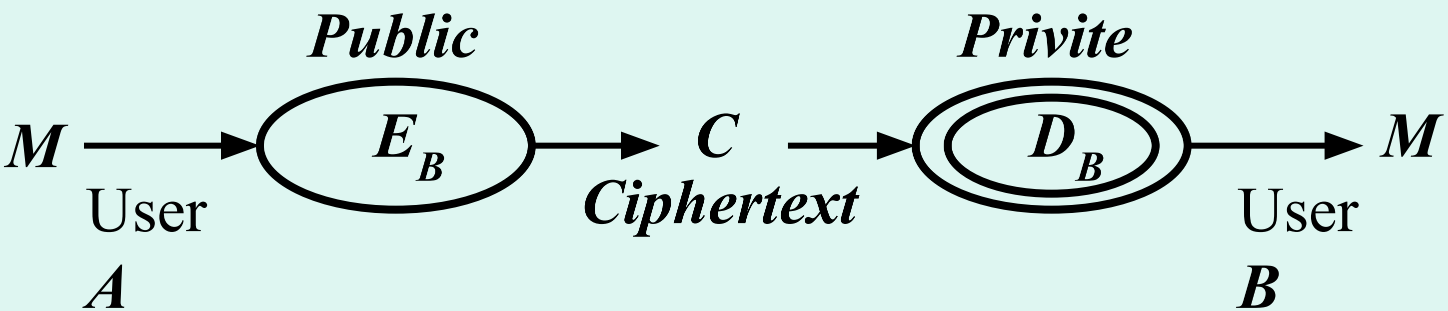

Fig.1.7. Secrecy in public-key system

For authenticity, $\boldsymbol{M}$ must be transformed by A's own private transformation $\boldsymbol{D}_A$. Ignoring secrecy for the moment, A sends $C=\boldsymbol{D}_A(\boldsymbol{M})$ to B. On receipt, B uses A's public transformation $\boldsymbol{E}_A$ to compute

$$\boldsymbol{E}_A(C)=\boldsymbol{E}_A(\boldsymbol{D}_A(\boldsymbol{M}))=\boldsymbol{M}$$

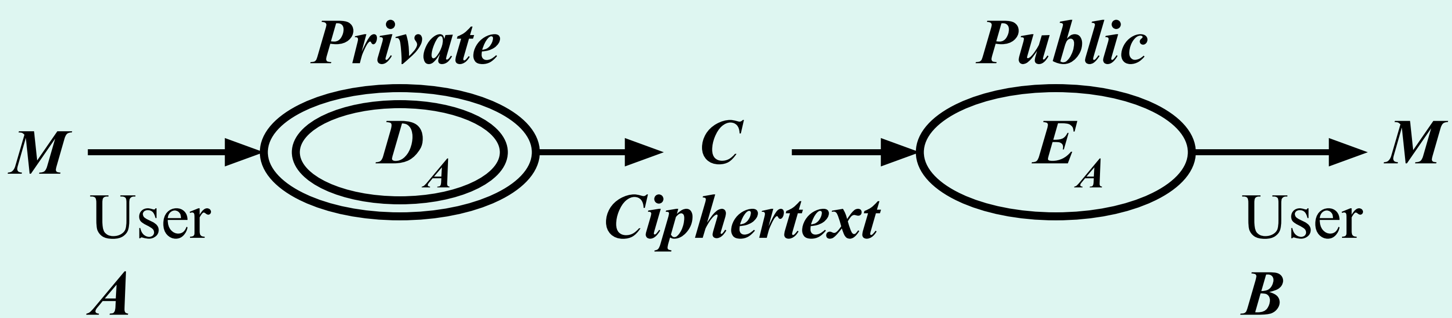

Fig.1.8. Authenticity in public-key system

Introduction

Public Key Cryptosystems

To achieve both secrecy and authenticity, the sender and receiver must each apply two sets of transformations. Sender A generates a ciphertext $C=\mathbf{E}_B(\mathbf{D}_A(M))$, and B recovers M according to

$$\mathbf{E}_A(\mathbf{D}_B(C))=\mathbf{E}_A(\mathbf{D}_B(\mathbf{E}_B(\mathbf{D}_A(M))))=\mathbf{E}_A(\mathbf{D}_A(M))=M.$$

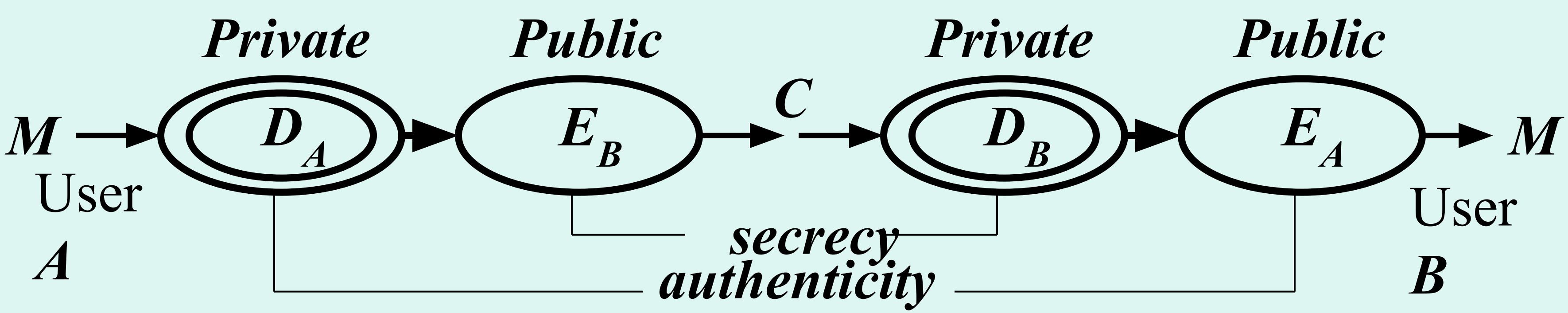

Fig.1.9. Secrecy and Authenticity in public-key system