信息论与编码

Information Theory and Coding

西南交通大学

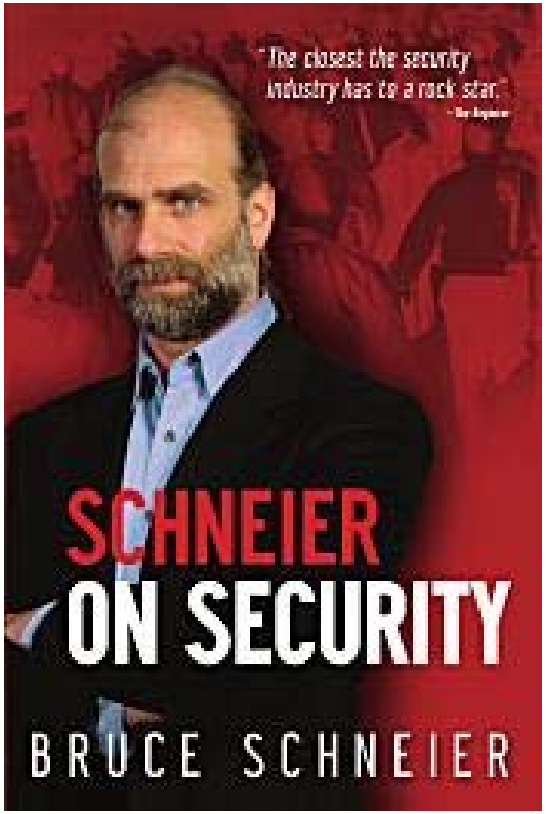
电子信息工程专业

2020

第6章 密码学

"it is insufficient to protect ourselves with laws; we need to protect ourselves with mathematics."

Bruce Schneier



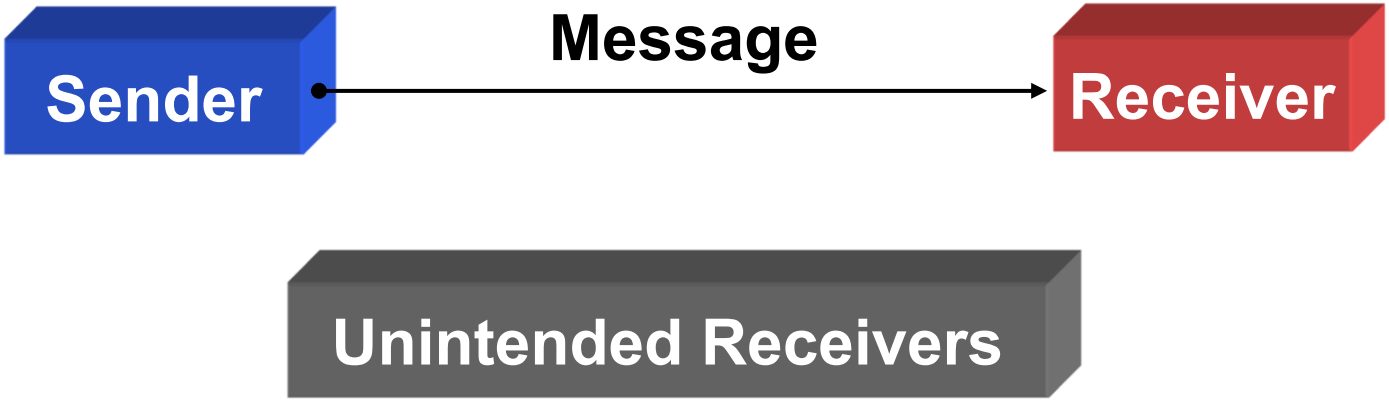
第6章 密码学

6-1 基础知识

专业术语：

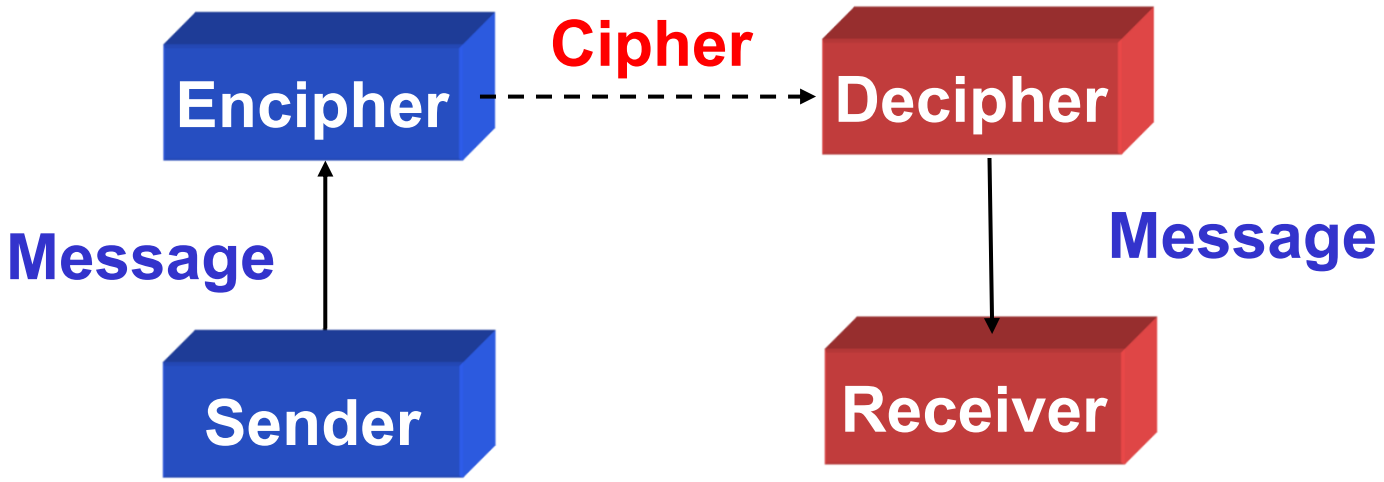
【1】发送者和接收者

假设发送者（sender）想发送消息给接收者（receiver），且想安全地发送消息：她确信窃听者不能阅读发送的消息。



第6章 密码学

【2】消息和加密



消息（message）被称为明文（plaintext）

用某种方法伪装消息以隐藏它的内容的过程称为加密（encryption）

被加密的消息称为密文（ciphertext）

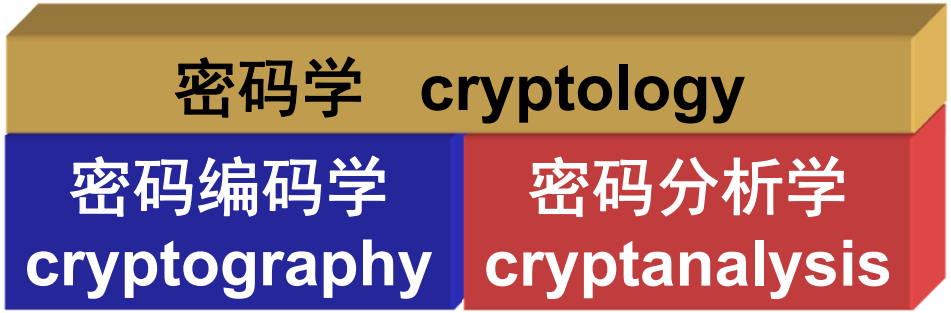
而把密文转变为明文的过程称为解密（decryption）

第6章 密码学

- 密码学（cryptology）

- 使消息保密的技术和科学叫做密码编码学（cryptography）
- 从事此行业的叫做密码编码者（cryptographer）

- 密码分析者（cryptanalyst）是从事密码分析的专业人员
- 密码分析学（cryptanalysis）就是破译密文的科学和技术



第6章 密码学

【3】鉴别、完整性和抗抵赖

除了提供机密外，密码学通常还具有其他作用：

鉴别（authentication） 消息的接收者应该能够确认消息的来源；入侵者不可能伪装成他人。

完整性（integrity） 消息的接收者应该能够验证在传送过程中消息没有被修改；入侵者不可能用假消息替代合法消息。

抗抵赖（nonrepudiation） 发送者不能事后虚假的否认它发送的消息。

第6章 密码学

【4】算法和密钥

密码算法（algorithm）也叫密码（cipher），是用于加密和解密的数学函数。（通常情况下有两个相关的函数，一个用来加密，一个用来解密）

加密函数E作用于消息M得到密文C，数学公式描述如下：

$$E(M)=C$$

解密函数D作用于密文C得到明文M，数学公式描述如下：

$$D(C)=M$$

$$D(E(M))=M$$

第6章 密码学

如果算法的保密性是基于保持算法的秘密，这种算法称为**受限制的（restricted）算法**。

问题：大的组织不能使用这种受限制的算法；

不能进行质量跟踪和标准化；

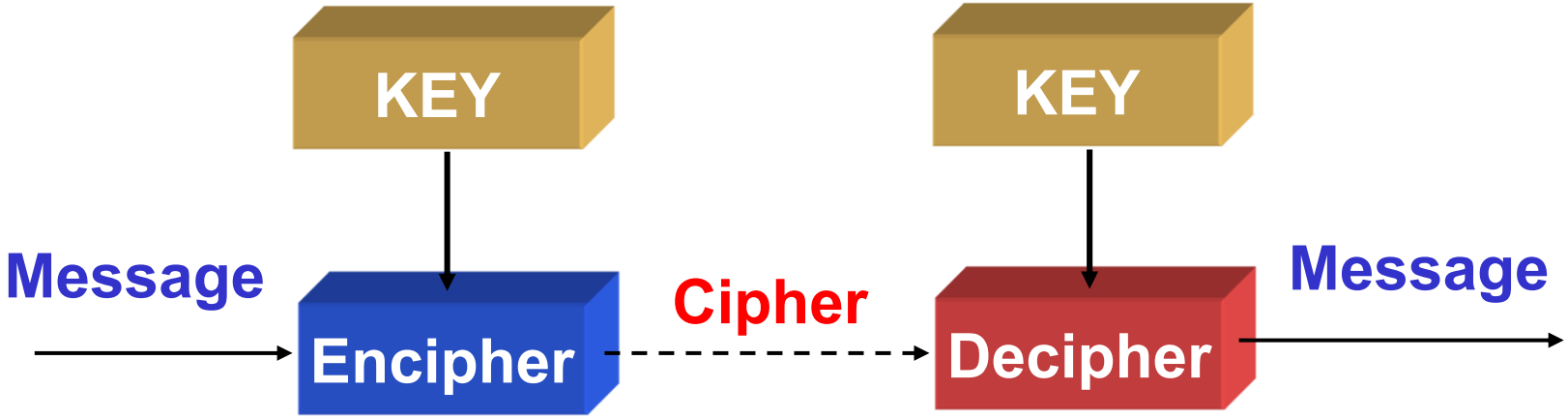
第6章 密码学

密钥(KEY)用K表示

密钥的取值范围称为密钥空间(keyspace)

(1) **对称密码体制**：加密和解密运算都采用相同的密钥

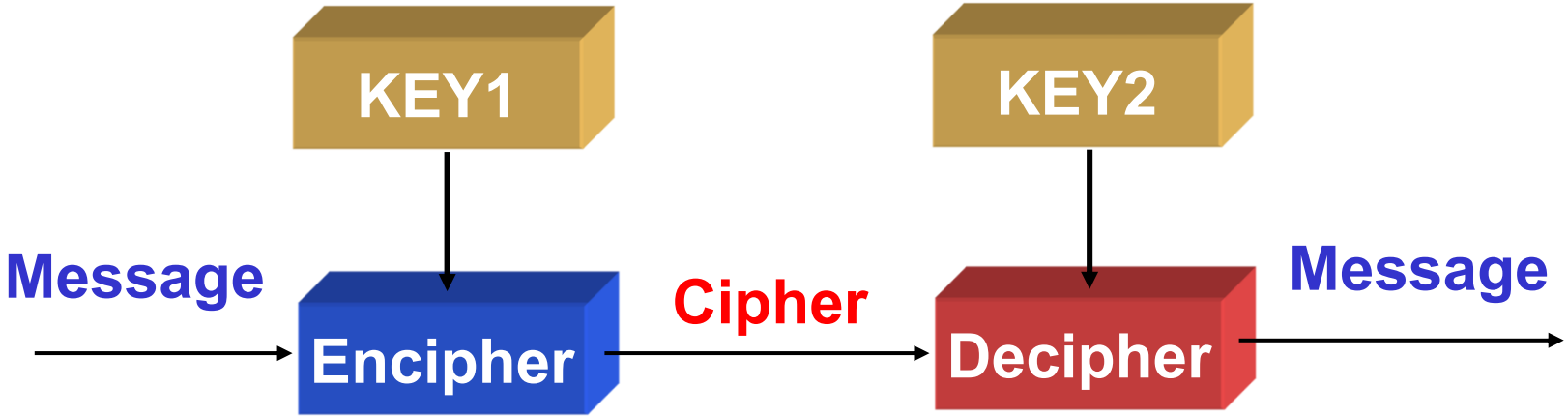
加/解密函数：$E_K(M)=C$　$D_K(C)=M$　$D_K(E_K(M))=M$



第6章 密码学

(2)非对称密码体制: 加密和解密运算采用不同的密钥

加/解密函数： $E_{K1}(M)=C$ $D_{K2}(C)=M$ $D_{K2}(E_{K1}(M))=M$



以上密钥的算法的安全性都是基于**密钥的安全性**；

而不是基于算法的细节的安全性；

密码系统由算法以及所有的可能的明文、密文和密钥组成；

第6章 密码学

【5】对称算法和公开密钥算法

(1)对称算法（**symmetric algorithm**）有时又叫传统密码算法，就是加密密钥能够从解密密钥推算出来，反过来也成立。在大多数对称算法中，加/解密密钥是相同的；

对称算法可以分为两类：

a.一次只对明文中的单个位（有时对字节）运算的算法称为序列算法（stream algorithm）或序列密码（stream cipher）。

b.一次对明文的一组位进行运算，这些位称为分组（block），相应的算法称为分组算法（block algorithm）或分组密码（block cipher）。

第6章 密码学

(2)公开密钥算法（**public-key algorithm**，也叫非对称算法）是这样设计的：用作加密的密钥不同于用作解密的密钥，而且解密密钥不能根据加密密钥计算出来（至少在合理假定的长时间内）。

之所以叫做公开密钥算法，是因为加密密钥能够公开，即陌生者能用加密密钥加密信息，但只有用相应的解密密钥才能解密信息。在这些系统中，加密密钥叫做公开密钥（public key），解密密钥叫做私人密钥（private key）。

第6章 密码学

6-2 密码协议

协议（protocol）是一系列步骤，包括两方或者多方，设计它的目的是要完成一系列的任务。

可见：协议是从开始到结束的一个序列，每一步必须依次执行，在前面一步完成之前，后面的步骤不能执行；完成一个协议要多方，单独一方不算协议；协议还必须完成完成一个任务。

特点：

1、每一方都必须了解协议，并预先知道所要完成的步骤；

2、每一方都必须同意并遵守协议；

3、协议必须清楚，每一步必须明确定义，不会引起误会；

4、协议必须完整，对每种可能情况必须规定具体动作。

第6章 密码学

6-2 密码协议

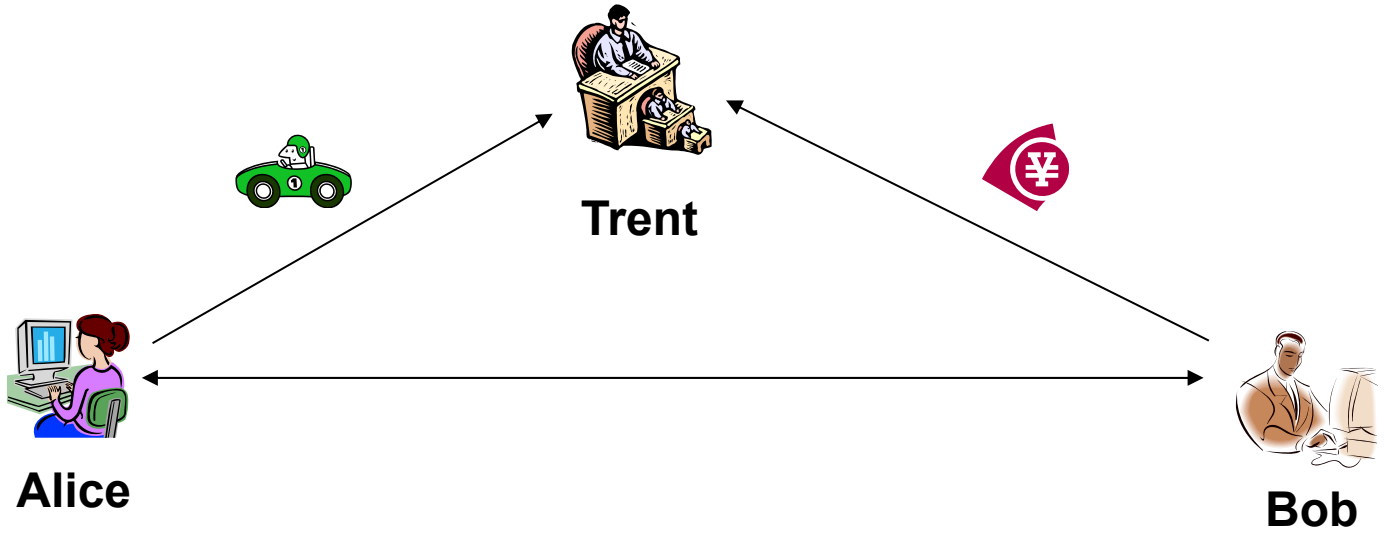
密码协议（cryptographic protocol）是使用密码学的协议。参与该协议的伙伴可能是朋友和完全信任的人，或者也可能是敌人和互相完全不信任的人。

密码协议包含某种密码算法，但是通常协议的目的不仅仅是为了简单的秘密性，在协议中使用密码的目的是防止或者发现窃听者和欺骗。

第6章 密码学

【1】 仲裁协议

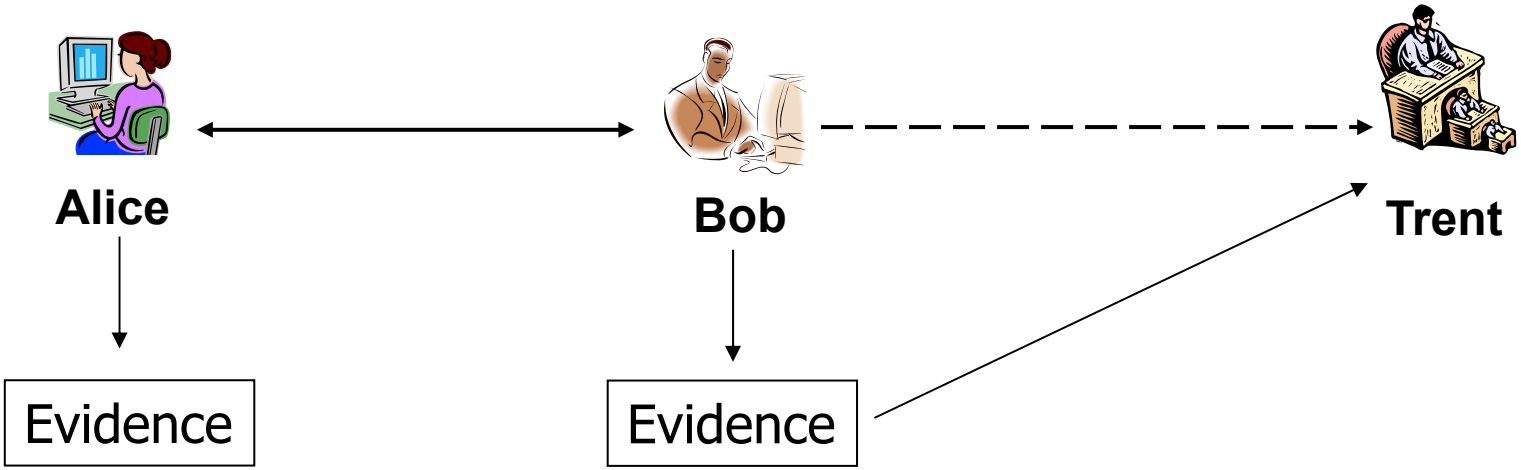
仲裁者是在完成协议的过程中，值得信任的公正的第三方，“公正”意味着仲裁者在协议中没有既得利益，对参与协议的任何人也没有特别的利害关系。
仲裁者能帮助互不信任的双方完成协议。



第6章 密码学

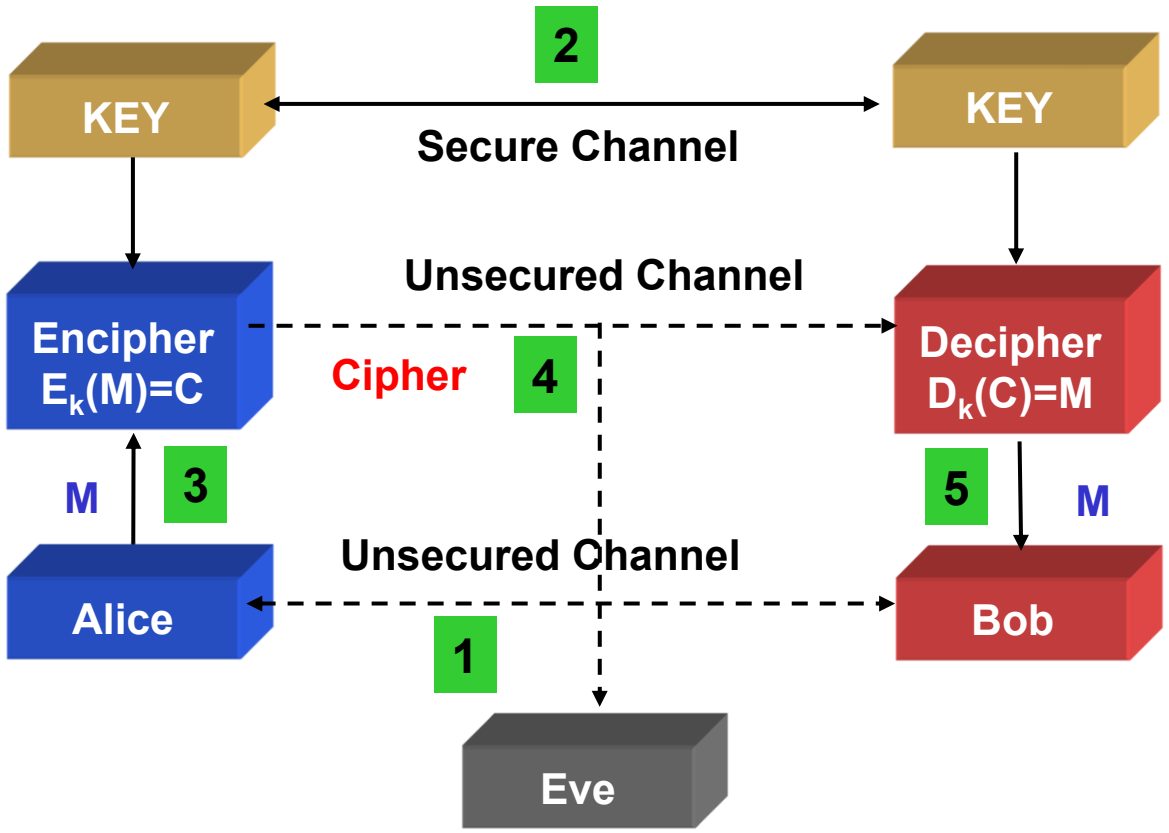
【2】 裁决协议

仲裁协议可以分成两个低级的子协议：一个是非仲裁子协议，执行协议的各方每次想要完成的。另外一个是仲裁子协议，仅在例外的情况下，即有争议的时候才执行，这种特殊的仲裁者叫做裁决人。



第6章 密码学

【3】 使用对称密码学通信



(1)Alice Bob协商用同一个密码系统

(2) Alice Bob协商用同一个密钥K

(3) Alice用加密算法和选取的密钥K加密她的明文消息M，得到了密文C

(4) Alice发送密文C给Bob

(5) Bob用同样的密钥K解密密文C，然后看到全部消息M

第6章 密码学

使用对称密码学通信存在的问题：

(a)密钥必须秘密的分配，它们比任加密的消息更有价值；

(b)如果密钥被损坏了，攻击者就能解密所有消息，并可以假装是其中一方；

(c)假设网络中每对用户使用不同的密钥，密钥总数随着用户的数量的增加而迅速增加。

N个用户的网络需要num＝N*(N-1)/2个密钥

第6章 密码学

【4】单项函数和单向散列函数

单向函数(One-way Function)

是公开密钥密码的中心；

单向函数计算起来相对容易，但求逆却非常难;

陷门单向函数(trapdoor one-way function)，如果你知道秘密，就很容易求逆;

单向散列函数(One-way Hash Function)

是现代密码学的中心；

散列函数就是将可变输入长度串(预映射)转换称为固定长度输出串(叫做散列值)的一种函数；

单向散列函数就是在一个方向上工作的散列函数；

可以看作是一个指纹，如果散列值相同，那么源数据肯定没有被修改；

第6章 密码学

Md5Checker Download Features How To Screenshots What's New

Latest Version: 3.3

- What's new
- Download

What is Md5Checker?

Md5Checker is a free, faster, lightweight and easy-to-use tool to manage, calculate and verify MD5 checksum of multiple files/folders (Screenshots):

- Calculate and display MD5 checksum of multiple files at one time.
- Use MD5 checksum to fleetly verify whether files have been changed.
- Load, save, add, remove and update MD5 checksum conveniently.
- It is about 300 KB and does not require any installation (portable).

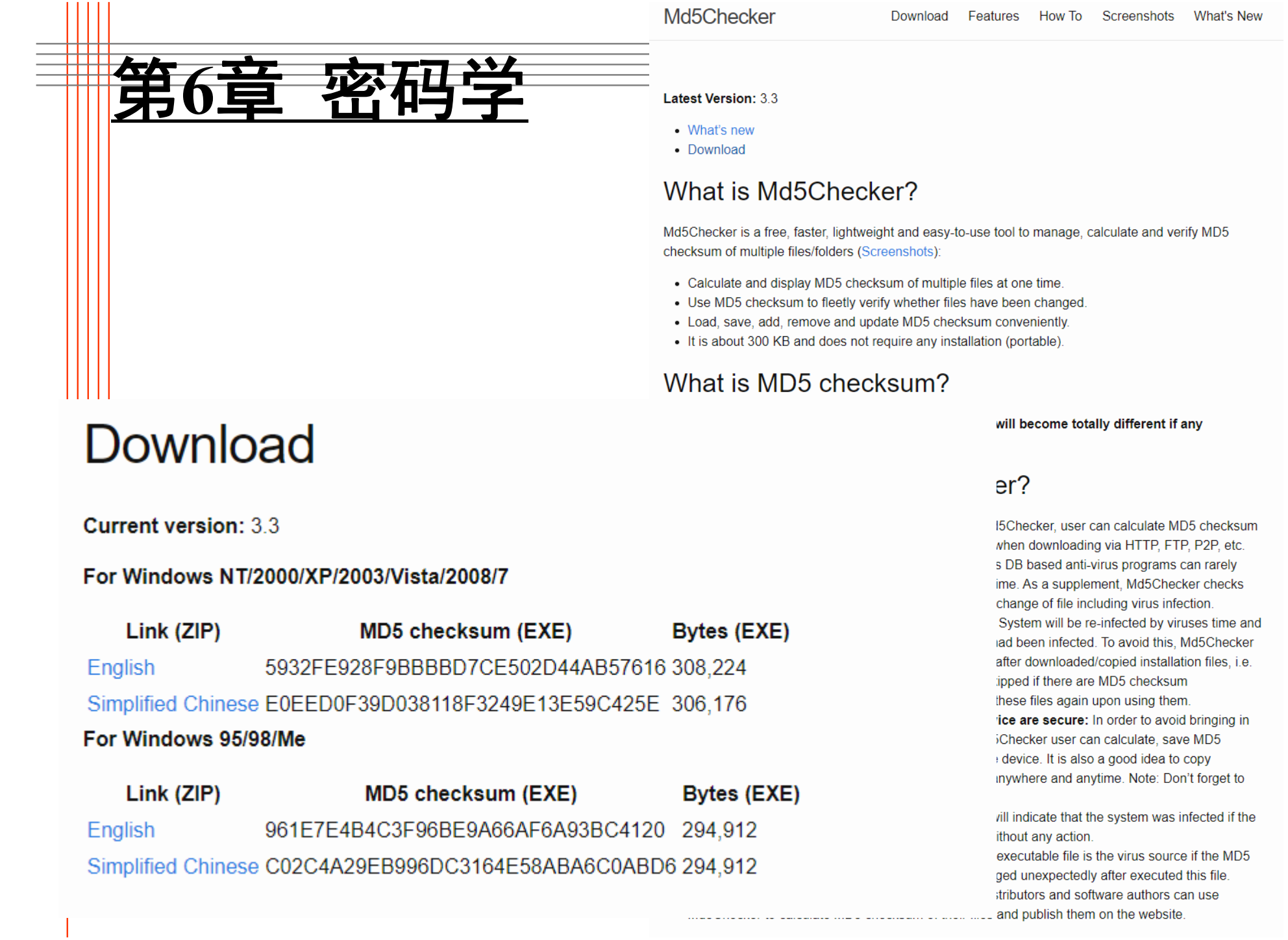
What is MD5 checksum?

MD5 checksum (MD5 hash) is a type of digests of files. **It will become totally different if any modification has been made to the file, even a byte.**

Why should I use Md5Checker?

1. **To verify the integrity of downloaded files:** With Md5Checker, user can calculate MD5 checksum of downloaded files and compare them with provided when downloading via HTTP, FTP, P2P, etc.
2. **To detect unknown viruses:** Only-for-existing-viruses DB based anti-virus programs can rarely detect all emerged new (i.e. not in the DB) viruses in time. As a supplement, Md5Checker checks whether files are original. By that user can detect any change of file including virus infection.
3. **To make sure that the installation files are secure:** System will be re-infected by viruses time and again while reinstalling software if the installation file had been infected. To avoid this, Md5Checker user can calculate and save the MD5 checksum right after downloaded/copied installation files, i.e. make sure these files are original (This step can be skipped if there are MD5 checksum downloaded/copied along with these files), and verify these files again upon using them.
4. **To make sure that files in a removable storage device are secure:** In order to avoid bringing in viruses from using the removable storage device, Md5Checker user can calculate, save MD5 checksum in advance and verify files afterwards in the device. It is also a good idea to copy Md5Checker into the device to be able to check files anywhere and anytime. Note: Don't forget to check the copied Md5Checker.
5. **To check out the security status of the system:** It will indicate that the system was infected if the MD5 checksum of one executable file was changed without any action.
6. **To find out the virus source:** It will indicate that one executable file is the virus source if the MD5 checksum of other several executable files have changed unexpectedly after executed this file.
7. **To calculate MD5 checksum for publishing:** File distributors and software authors can use Md5Checker to calculate MD5 checksum of their files and publish them on the website.

第6章 密码学



Md5Checker Download Features How To Screenshots What's New

Latest Version: 3.3

- What's new
- Download

What is Md5Checker?

Md5Checker is a free, faster, lightweight and easy-to-use tool to manage, calculate and verify MD5 checksum of multiple files/folders (Screenshots):

- Calculate and display MD5 checksum of multiple files at one time.
- Use MD5 checksum to fleetly verify whether files have been changed.
- Load, save, add, remove and update MD5 checksum conveniently.
- It is about 300 KB and does not require any installation (portable).

What is MD5 checksum?

will become totally different if any

er?

l5Checker, user can calculate MD5 checksum
when downloading via HTTP, FTP, P2P, etc.
s DB based anti-virus programs can rarely
ime. As a supplement, Md5Checker checks
change of file including virus infection.
System will be re-infected by viruses time and
ıad been infected. To avoid this, Md5Checker
after downloaded/copied installation files, i.e.
ipped if there are MD5 checksum
these files again upon using them.
ice are secure: In order to avoid bringing in
Checker user can calculate, save MD5
device. It is also a good idea to copy
ınywhere and anytime. Note: Don't forget to

ill indicate that the system was infected if the
ithout any action.
executable file is the virus source if the MD5
ged unexpectedly after executed this file.
tributors and software authors can use
and publish them on the website.

Download

Current version: 3.3

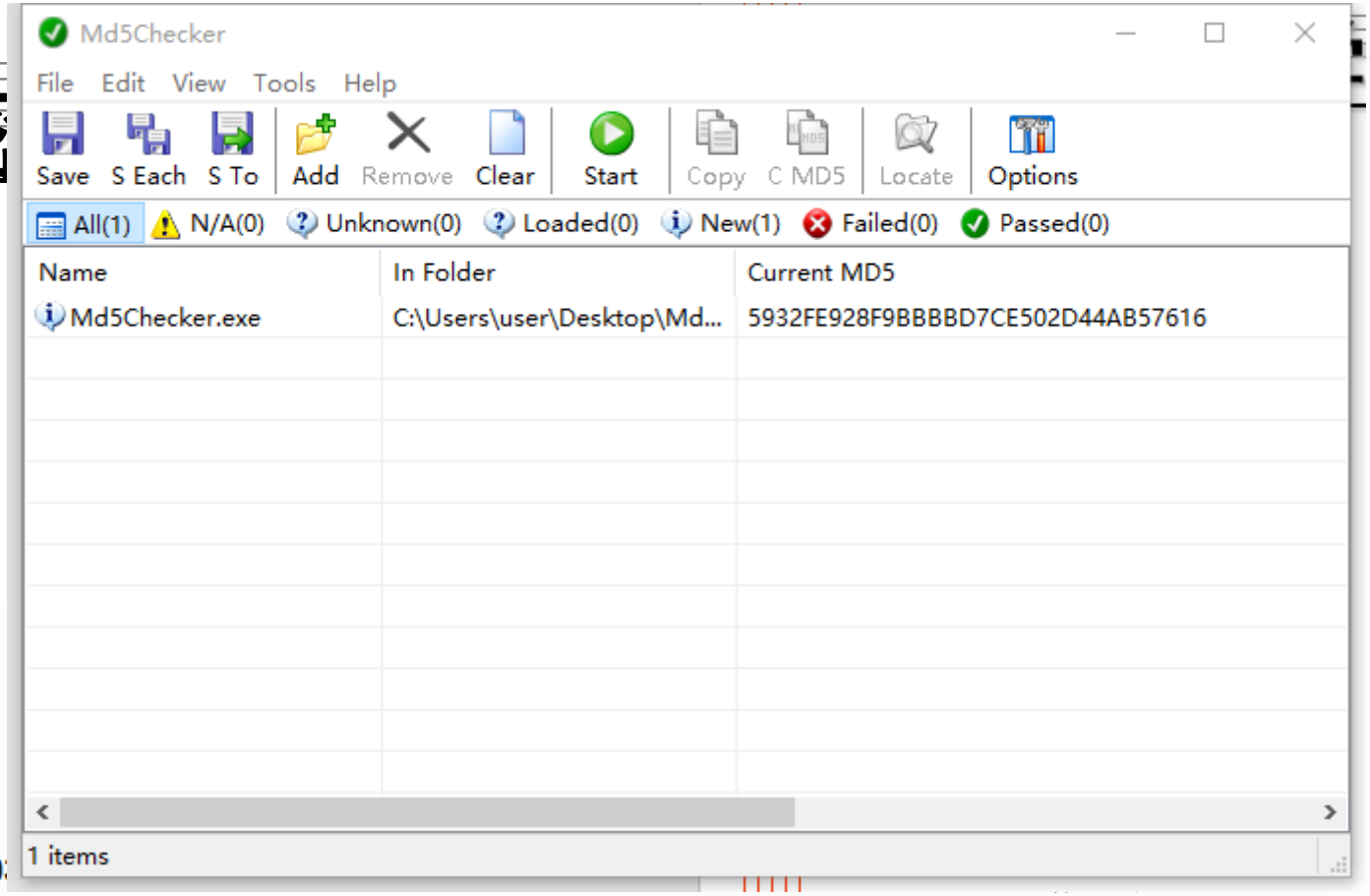
For Windows NT/2000/XP/2003/Vista/2008/7

Link (ZIP)	MD5 checksum (EXE)	Bytes (EXE)
English	5932FE928F9BBBBD7CE502D44AB57616	308,224
Simplified Chinese	E0EED0F39D038118F3249E13E59C425E	306,176

For Windows 95/98/Me

Link (ZIP)	MD5 checksum (EXE)	Bytes (EXE)
English	961E7E4B4C3F96BE9A66AF6A93BC4120	294,912
Simplified Chinese	C02C4A29EB996DC3164E58ABA6C0ABD6	294,912

第6章 密



Download

Current version: 3.3

For Windows NT/2000/XP/200

Link (ZIP)	MD5 checksum (EXE)	Bytes (EXE)
English	5932FE928F9BBBBD7CE502D44AB57616	308,224
Simplified Chinese	E0EED0F39D038118F3249E13E59C425E	306,176

For Windows 95/98/Me

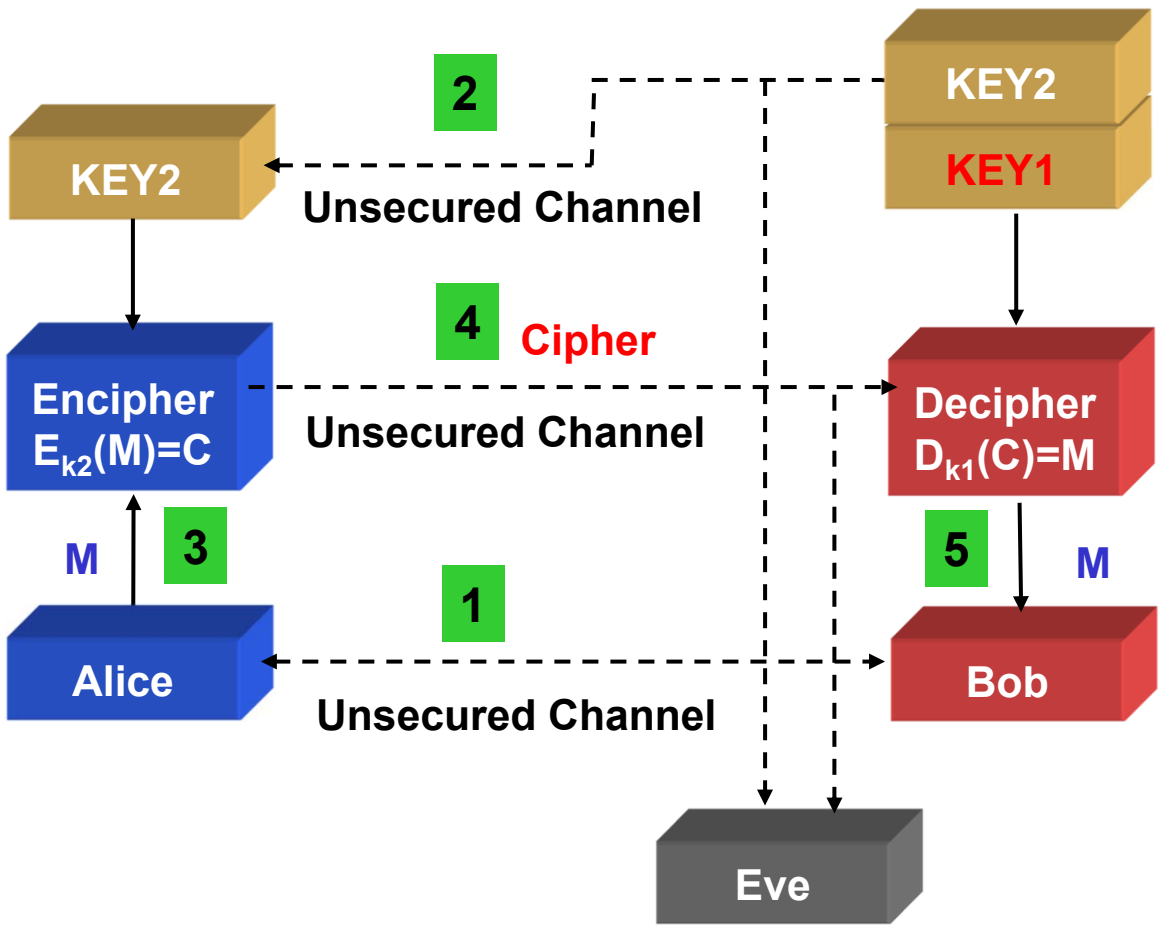
Link (ZIP)	MD5 checksum (EXE)	Bytes (EXE)
English	961E7E4B4C3F96BE9A66AF6A93BC4120	294,912
Simplified Chinese	C02C4A29EB996DC3164E58ABA6C0ABD6	294,912

change of file including virus infection.
System will be re-infected by viruses time and
ıad been infected. To avoid this, Md5Checker
after downloaded/copied installation files, i.e.
ıpped if there are MD5 checksum
these files again upon using them.
ice are secure: In order to avoid bringing in
Checker user can calculate, save MD5
device. It is also a good idea to copy
ınywhere and anytime. Note: Don't forget to

ıill indicate that the system was infected if the
ithout any action.
executable file is the virus source if the MD5
ged unexpectedly after executed this file.
ıtributors and software authors can use
and publish them on the website.

第6章 密码学

【5】 使用公钥密码学通信



(1)Alice Bob协商用同一个公开密钥密码系统

(2)Bob将他的公开密钥K2传给Alice

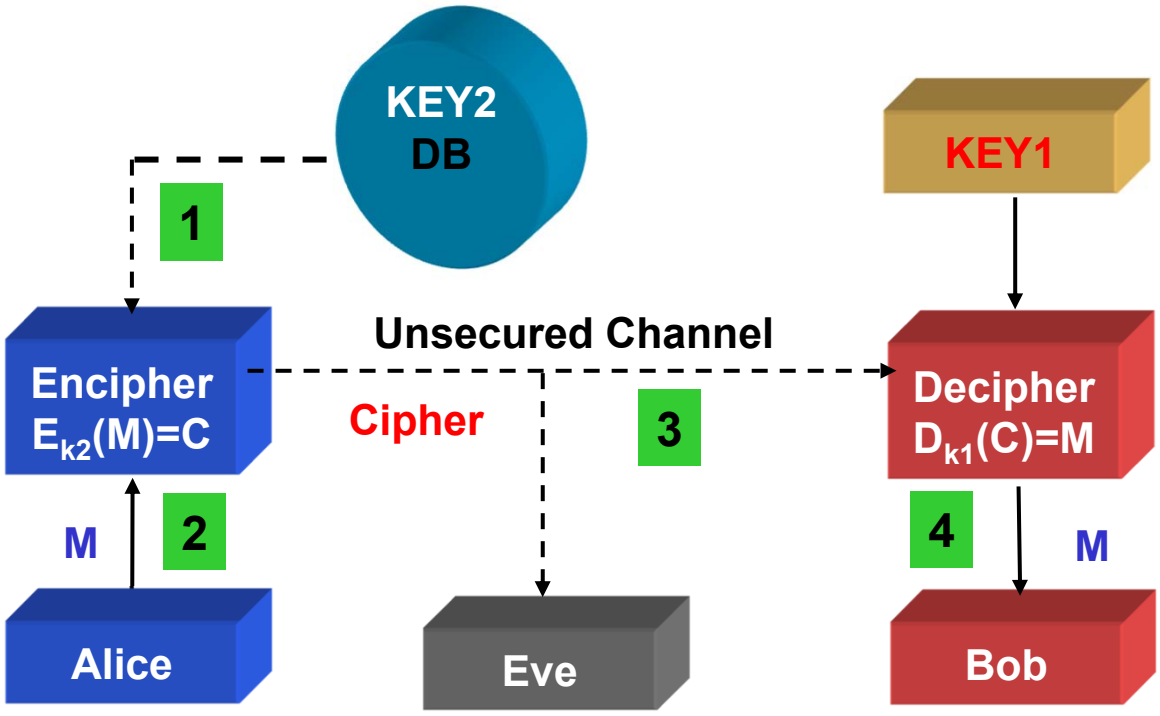
(3) Alice用Bob给她的公开密钥K2对消息M加密成为密文C

(4) Alice将加密后的密文C传给Bob

(5) Bob用他的私人密钥K1对Alice的密文C进行解密得到Alice的消息原文M

第6章 密码学

使用公钥密码学通信



(1)Alice 从数据库中的得到Bob的公开密钥K2

(2) Alice用Bob的公开密钥K2对消息M加密成为密文C

(3) Alice将加密后的密文C传给Bob

(4) Bob用他的私人密钥K1对Alice的密文C进行解密得到Alice的消息原文M

第6章 密码学

【6】 数字签名(Digital Signature)

现实世界签名：

1、签名是可信的。

2、签名不可伪造。

3、签名不可重用。

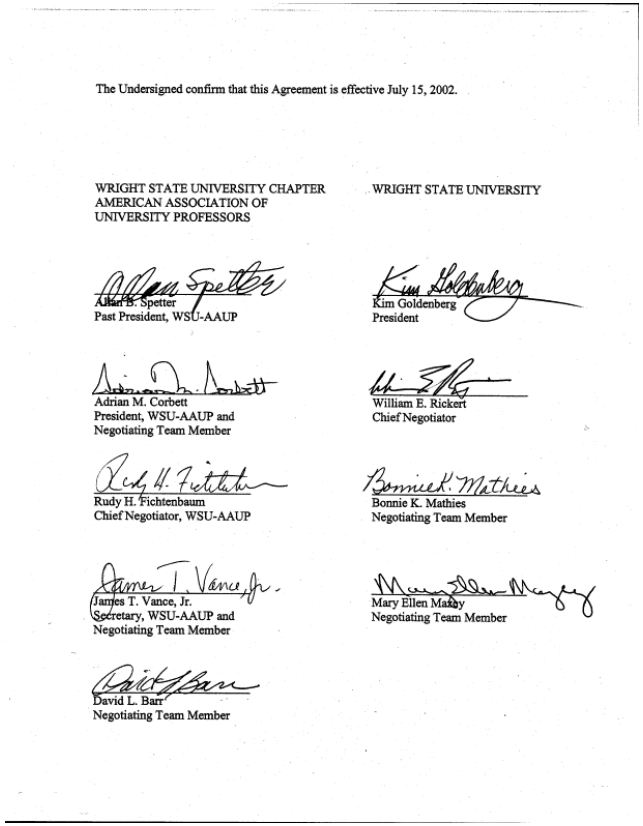
4、签名后的文件不可改变。

5、签名是不可抵赖的。

实际上：签名可伪造、签名后的文件可以被修该……

但是：我们仍然愿意用签名，因为欺骗是困难的，还要冒被发现的风险

计算机上如何采用签名？



The Undersigned confirm that this Agreement is effective July 15, 2002.

WRIGHT STATE UNIVERSITY CHAPTER
AMERICAN ASSOCIATION OF
UNIVERSITY PROFESSORS

Allen B. Spetter
Past President, WSU-AAUP

Adrian M. Corbett
President, WSU-AAUP and
Negotiating Team Member

Rudy H. Fichtenbaum
Chief Negotiator, WSU-AAUP

James T. Vance, Jr.
Secretary, WSU-AAUP and
Negotiating Team Member

David L. Barr
Negotiating Team Member

WRIGHT STATE UNIVERSITY

Kim Goldenberg
President

William E. Rickert
Chief Negotiator

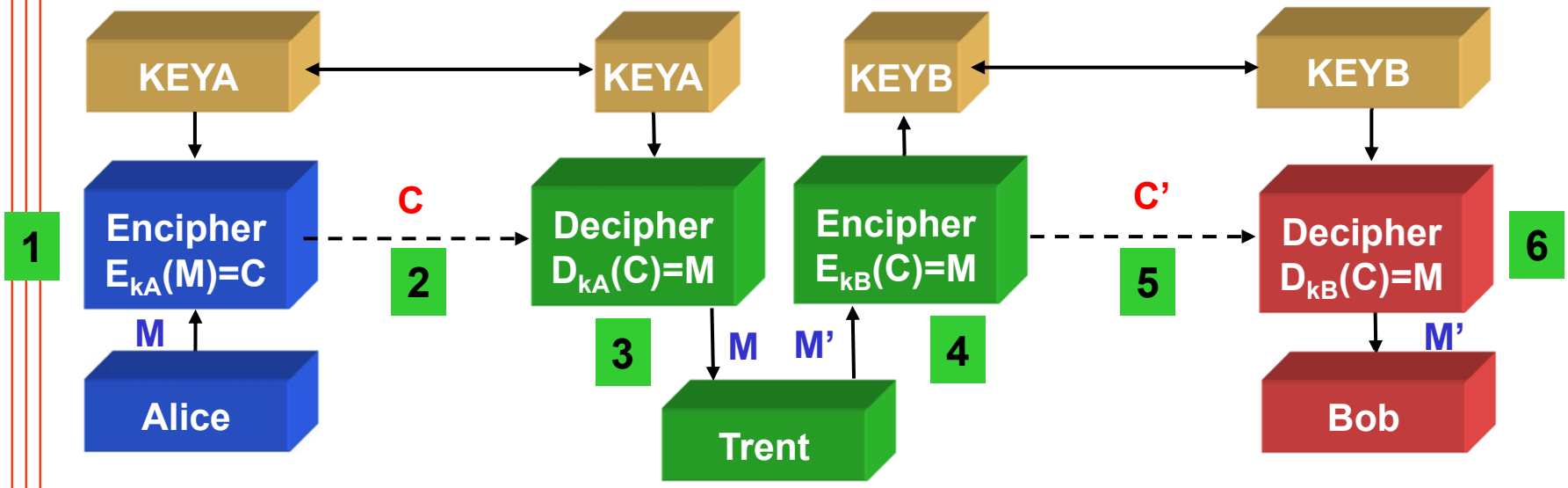
Bonnie K. Mathies
Negotiating Team Member

Mary Ellen Mazey
Negotiating Team Member

第6章 密码学

【6】 数字签名(Digital Signature)

(a) 使用对称密码系统和仲裁者对文件签名

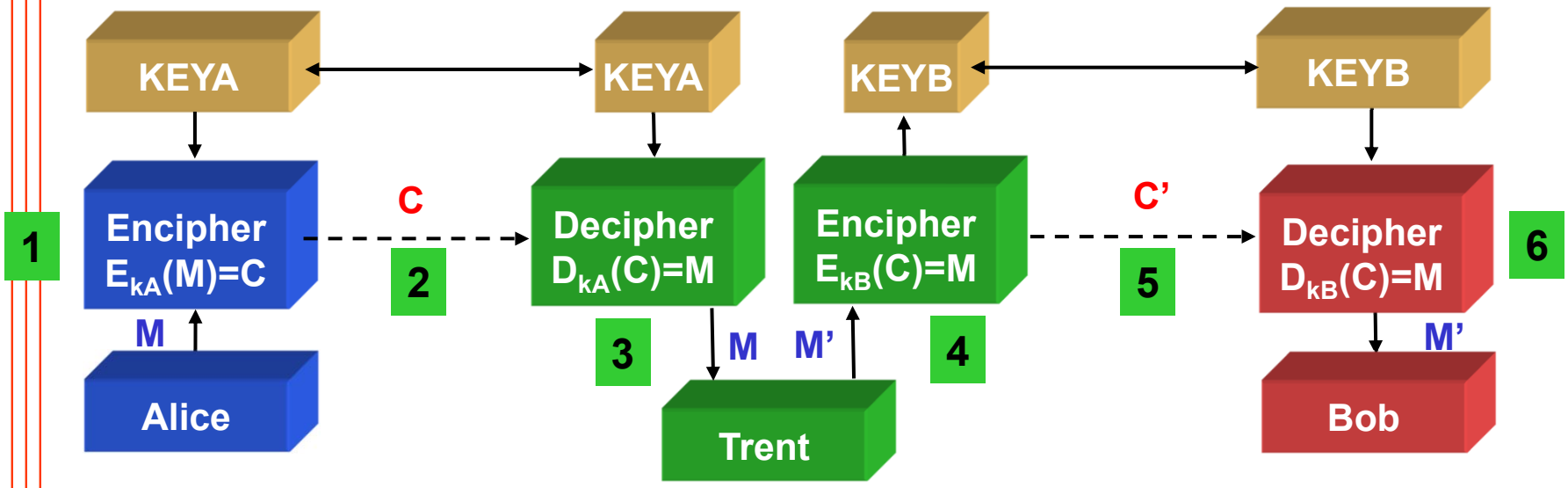


(1)Alice 用KA加密她准备发送给Bob的文件M (2)Alice将加密后的密文C发送给仲裁者Trent (3)Trent用KA解密文件密文C (4)Trent将这个解密文件M和他收到Alice的文件的声明，一起用KB加密为密文C' (5) Trent将加密的密文C'发送给Bob (6)Bob用KB解密文件密文C'，他得到了Alice发出的文件M和Trent的证书，证明文件来自Alice

第6章 密码学

【6】 数字签名(Digital Signature)

(a) 使用对称密码系统和仲裁者对文件签名



存在问题：

仲裁者不得不每天加密、解密消息，它是系统瓶颈；

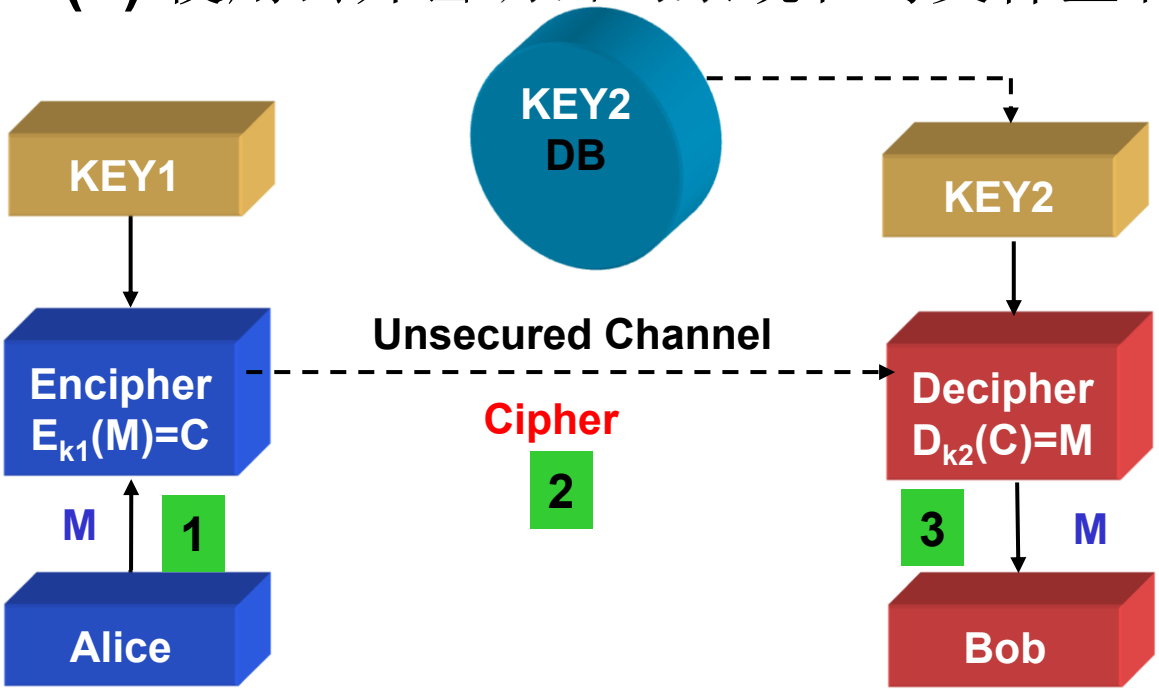
仲裁者必须完美无缺，不能犯一次错误；

仲裁者手中的密钥数据库必须安全。

第6章 密码学

【6】 数字签名(Digital Signature)

(b) 使用公开密钥密码系统和对文件签名



(1)Alice 用她的私人密钥K1对文件M加密

(2)Alice将加密后的密文C发送给Bob

(3)Bob用Alice的公开密钥K2解密文件密文C，从而验证Alice的签名

使用公开密钥密码系统和对文件签名

该签名特点：可以实现该签名是可信的，不可伪造的，不可重用的，签名后文件是不可改变的，签名是不可抵赖的。

第6章 密码学

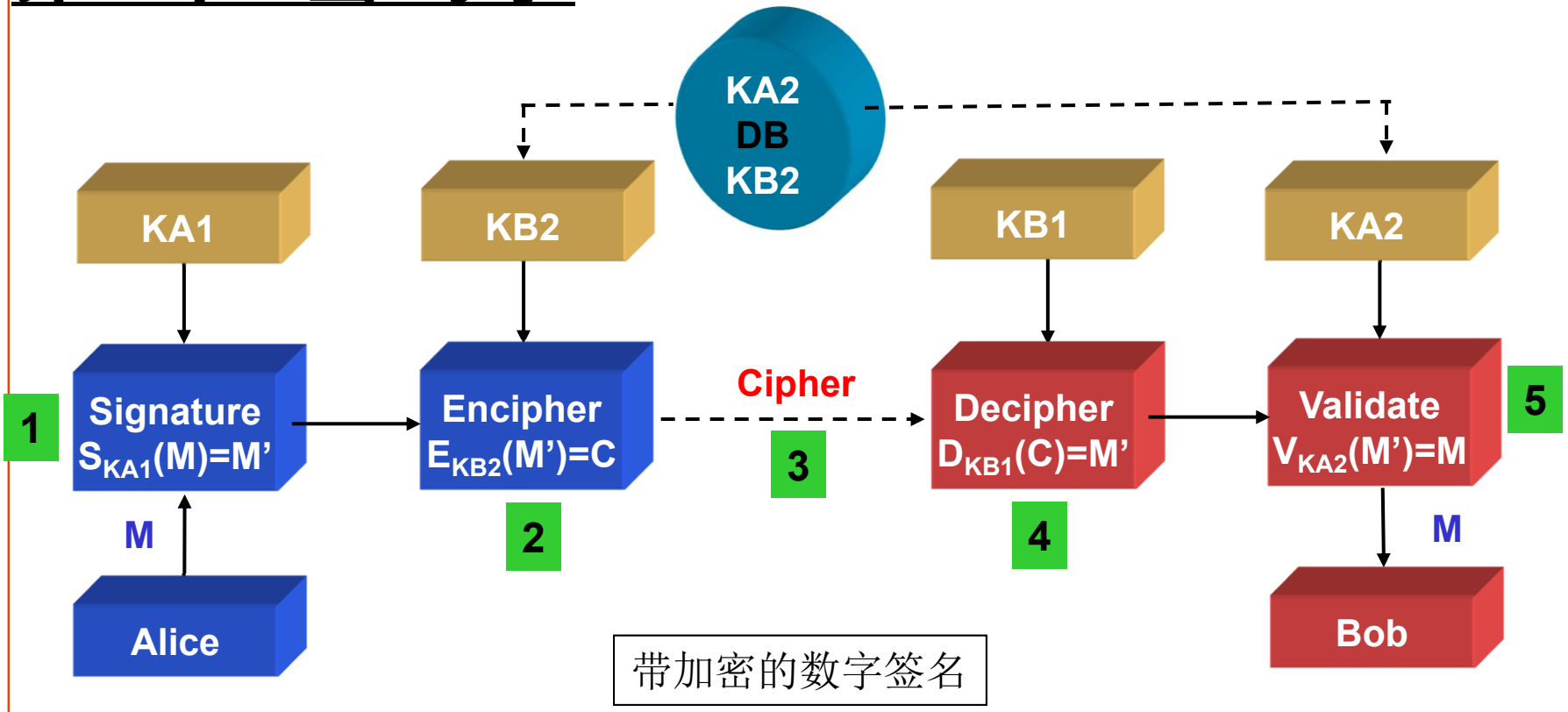
用私人密钥K对消息进行签名可表示为$S_K(M)$
用相应的公开密钥验证消息可以表示为$V_K(M)$

签名时附在文件上的位串叫做数字签名(Digital Signature)
消息的接收者用以确认发送者的身份和消息的完整性的整个协议称为鉴别(Validate)；

【7】 带加密的数字签名

通过将公开密钥密码和数字签名结合起来，能够产生一个将数字签名的真实性和加密的安全性结合起来的协议：

第6章 密码学



带加密的数字签名

(1) Alice 用她的私人密钥KA1对文件M签名，得到签名后消息M'
(2) Alice用Bob的公开密钥KB2将签名后消息加密 $C=E_{KB2}(S_{KA1}(M))$
(3) Alice将上述操作后得到的密文C发送给Bob
(4) Bob用他的私人密钥KB1解密密文C得到签名后消息M'
(5) Bob用Alice的公开密钥KA2验证并恢复出文件M $M=V_{KA2}(D_{KB1}(C))$

第6章 密码学

6-3 密码分析

密码分析学是在不知道密钥的情况下，恢复出明文的科学。
密码分析也可以发现密码体制的弱点。
常见的密码分析攻击有四类：

(1) 唯密文攻击（ciphertext-only attack） 密码分析者有一些密文，这些消息都是用一加密算法加密。

(2) 已知明文攻击（know-plaintext attack）密码分析这不仅可以得到一些消息的密文，而且也知道这些消息的明文。

(3) 选择明文攻击（chosen-plaintext attack）分析这不但可以得到一些消息的明文，而且它们可以选择被加密的明文。

(4) 自适应选择明文攻击（adaptive-chosen-plaintext attack）密法分析这不但能够选择被加密的明文，而且也能基于以前加密的结果修正这个选择。

第6章 密码学

6-4 算法的安全性

【1】破译算法可以分为不同的级别：

(1)全部破译（total break）找出密钥

(2)全部推导（global deduction）找出替代算法

(3)实例推导（instance deduction）找出明文

(4)信息推导（information deduction）获得一些有关密钥或明文的信息

【2】可以用不同的方式来衡量攻击方法的复杂性：

(1)数据复杂性（data complexity）用作攻击输入所需要的数据量

(2)处理复杂性（processing complexity）完成攻击所需要的时间

(3)存储需求（storage requirement）进行攻击所需要的数据量。

第6章 密码学

6-5 密码学的发展历史

【1】手工密码编码系统

Caesar Cipher(恺撒编码)

2000年前 Julius Caesar

Alphabet: **ABCDEFGHIJKLMNOPQRSTUVWXYZ**

Substitution: **DEFGHIJKLMNOPQRSTUVWXYZABC**

Plaint Text: "ROME SWEET ROME"

Cipher: "URPH VZHHW URPH"

第6章 密码学

Substitutions & Permutations (替代和换位)

Substitutions

Alphabet: **ABCDEFGHIJKLMNOPQRSTUVWXYZ**
Substitution: **QWERTYUIOPASDFGHJKLZXCVBNM**

Plaint Text: "SEND THE MATERIAL NOW"
Cipher: "LTFR ZIT DQZTKOQS FGV"

Permutations

S E N D T H
E M A T E R
I A L N O W

Plaint Text: "SENDTHEMATERIALNOW"
Cipher: "SEIEMANALDTNTEOHRW"

第6章 密码学

The Vigenère Cipher (维吉尼亚密码)1586

Blaise de Vigen re, a Frenchman who lived from 1523 to 1596.

【2】机械密码编码系统

Cipher Disks

Leon Battista Alberti in the 15th century.

The KRYHA Device

First appearing in the 1920 s, the KRYHA was invented by the Ukrainian, Alexander Von Kryha.

The KRYHA Device

这是一个多表加密设备，密钥长度为442，周期固定。一个由数量不等的齿的轮子引导密文轮不规则运动。

第6章 密码学

【3】机械电气密码编码系统

The ENIGMA(恩尼格码)

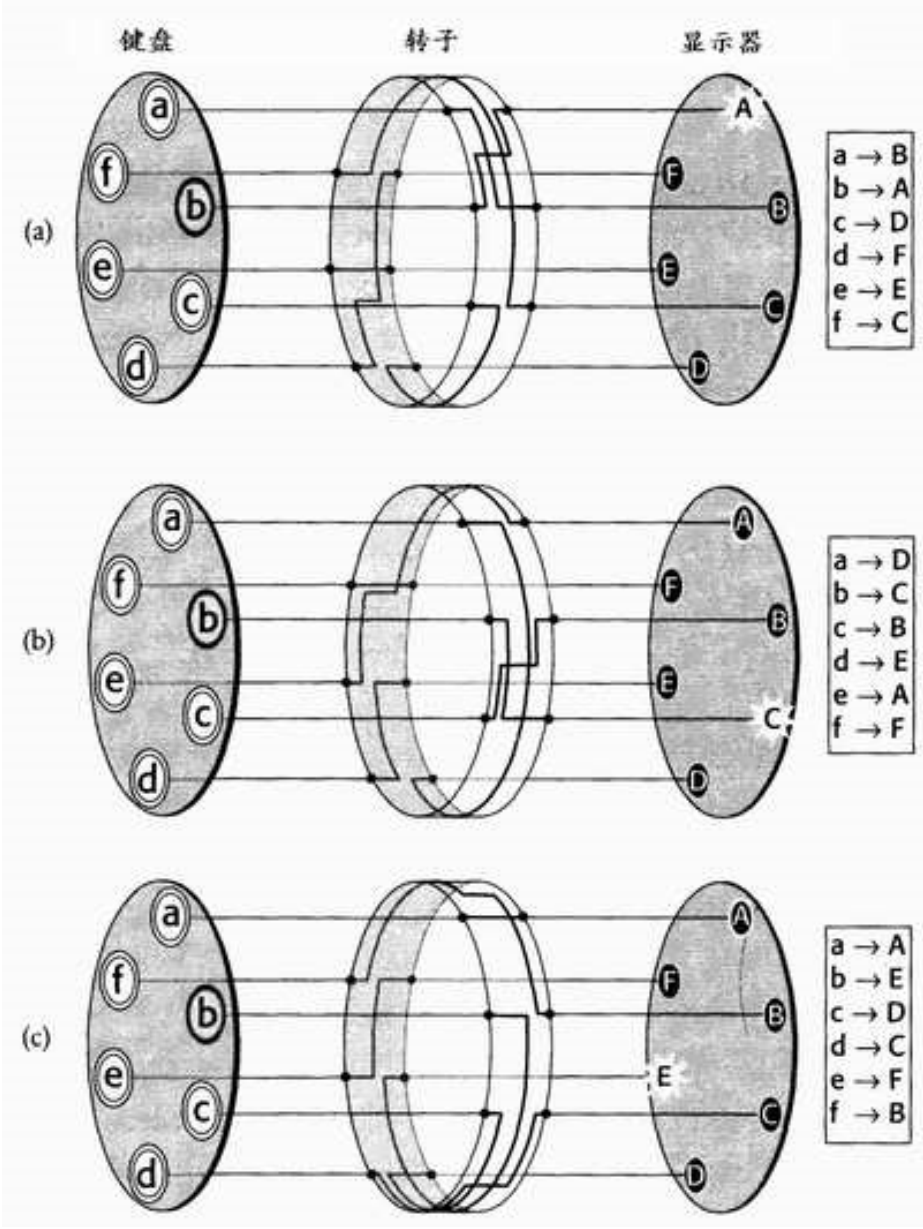
1918年，德国发明家亚瑟·谢尔比乌斯(Arthur Scherbius)和他的朋 友理查德·里特(Richard Ritter)发明的加密电子机械名叫ENIGMA

第6章 密码学

【3】机械电气密码编码系统

The ENIGMA(恩尼格码)

1918年，德国发明家亚瑟·谢尔比乌斯(Arthur Scherbius)和他的朋 友理查德·里特(Richard Ritter)发明的加密电子机械名叫ENIGMA



第6章 密码学

【4】现代密码编码系统

目前常见的计算机算法:

- DES (Data Encryption Standard)是最通用的计算机加密算法。DES是美国和国际标准，它是对称算法，加密和解密的密钥是相同的。(IBM设计，1977年开始使用，DES在替代和换位基础上发展的)
- IDEA (Int. Data Encryption Algorithm)国际数据加密算法 (由瑞士两科学家1990年提出)
- RSA (Rivest, Shamir, Adleman)是最流行的公开密钥算法，它能用作加密和数字签名 (MIT)
- DSA (Digital Signature Algorithm)是另外一种公开密钥算法，它不能用作加密，只能用作数字签名

第6章 密码学

参考书籍：

- Schneier, Bruce. *Applied Cryptography*, Wiley, (2nd Edition), 1996.
- Deavours, Cipher; Kahn, David; Kruh, Louis; Mellen, Greg; and Winkel, Brian.*Cryptology: Machines, History & Methods*, Artech House, 1989.
- Stinson, Doug. *Cryptography, Theory and Practice*, CRC Press, 4th Printing, 1996.

第6章 密码学

相关网站：

- Military Communications & Electronics Museum (Kingston, Ontario, Canada) http://www.c-and-e-museum.org/
- Bletchley Park (England): http://www.cranfield.ac.uk/CCC/BPark/
- National Crypto Logic Museum (Fort Meade, Maryland, USA)

http://www.nsa.gov:8080/museum/

- JAVA Applet Simulator of 3-rotor ENIGMA:

http://www.ugrad.cs.jhu.edu/~russell/classes/enigma/