中山大學
SUN YAT-SEN UNIVERSITY

Module I. Fundamentals of Information Security

Chapter 2
Cryptographic Techniques

Web Security: Theory & Applications

School of Data & Computer Science, Sun Yat-sen University

Outline

- **2.1 Cryptology Introduction**
  - Introduction
  - History
  - Concepts & Items
- **2.2 Symmetric Key Cryptographic Algorithms**
  - Introduction
  - Types & Modes
  - Data Encryption Standard (DES)
  - Advanced Encryption Standard (AES)

Outline

- **2.3 Mathematical Foundations of Public-Key Cryptography**
  - Prime factorizations of integers
  - The *Euclidean* Algorithm
  - *Bézout*'s Theorem
  - Linear Congruence
  - The Extended_*Euclidean* Algorithm
  - The Chinese Remainder Theorem
  - *Euler*'s φ function
  - *Euler*'s Theorem
  - *Fermat*'s Little Theorem

Outline

- **2.4 Asymmetric Key Cryptographic Algorithms**
  - Introduction
  - The RSA Algorithm
  - Digital Signatures
- **2.5 Hashing Algorithms**
  - Introduction
  - Message-Digest Algorithm (MD5)
- **2.6 Typical Applications**
  - MD5 and Passwords
  - AES and WiFi Protected Access
  - RSA and e-Business

2.1 Cryptology Introduction

2.1.1 Introduction

- **Definition**
  - **Cryptography** (or *cryptology*; from Greek kryptós, “hidden, secret”; and gráphein, “writing”, or *-logia*, “study”, respectively) is the practice and study of techniques for secure communication in the presence of third parties (called adversaries 敌手). More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation.

2.1 Cryptology Introduction

2.1.1 Introduction

- **Definition**
  - Modern Cryptography
    - ✧ Computational Hardness
      - ◌ Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary.
    - ✧ Computationally Secure
      - ◌ It is theoretically possible to break such a system, but it is infeasible to do so by any known practical means. These schemes are therefore termed computationally secure; theoretical advances, e.g., improvements in integer factorization algorithms, and faster computing technology require these solutions to be continually adapted.

2.1 Cryptology Introduction

2.1.1 Introduction

- **Definition**
  - Modern Cryptography
    - ✧ Computationally Secure
      - ◌ There exist information-theoretically secure schemes that provably cannot be broken even with unlimited computing power - an example is the one-time pad (OTP) - but these schemes are more difficult to implement than the best theoretically breakable but computationally secure mechanisms.
      - ◌ 破译的代价超出信息本身的价值
      - ◌ 破译的时间超出了信息的有效期

2.1 Cryptology Introduction

2.1.1 Introduction

- **Definition**
  - 密码学是研究如何隐密地传递信息的学科。
    - ***Cryptography*** 或 ***Cryptology*** 源于希腊语 *kryptós* “隐藏的”，和 *gráphein* “书写”。
    - 密码学是关于如何在敌人存在的环境中通讯。 - R. Rivest
    - 密码学的首要目的是隐藏信息的涵义，而并非隐藏信息的存在
    - 现代密码学由密码编码学 (Cryptography, 信息编码和隐蔽) 和密码分析学 (Crptanalisis， 信息破译和伪造) 两个分支学科构成，特指对信息以及其传输的数学性研究，通常被认为是数学、计算机科学和电子工程学的交叉学科，和信息论也密切相关。
    - 密码学是计算机与网络安全相关问题如认证、访问控制等的核心。

2.1 Cryptology Introduction

2.1.1 Introduction

- ***Kerckhoffs*' Principle**
  - In cryptography, *Kerckhoffs*' principle was stated by Dutch cryptographer *Auguste Kerckhoffs* in the 19th century: A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.
  - Originally, it is the second axiom of *Auguste Kerckhoffs'* six design principles for military ciphers - "It should not require secrecy, and it should not be a problem if it falls into enemy hands".

2.1 Cryptology Introduction

2.1.1 Introduction

- ***Shannon*'s Maxim**
  - *Kerckhoffs*‘ principle was reformulated (or perhaps independently formulated) by *Claude Shannon* as “the enemy knows the system”, i.e., “one ought to design systems under the assumption that the enemy will immediately gain full familiarity with them”. In that form, it is called *Shannon’s* maxim. In contrast to “security through obscurity (费解)", it is widely embraced by cryptographers.

2.1 Cryptology Introduction

2.1.1 Introduction

- ***Kerckhoffs* 原理**
  - 密码分析者知道双方使用的密码系统，包括明文的统计特性、加解密体制等，唯一不知道的是密钥。
    - ✧ 密码算法应该对外公开。一个密码系统需要保密的部分越多，可能的弱点也越多。
    - ✧ 密码系统的设计原则，应该是在 *Kerckhoffs* 原理下实现安全目标。

2.1 Cryptology Introduction

2.1.1 Introduction

- **密码分析**
  - 密码分析学研究如何在未知密钥的情况下恢复明文。
  - 密码分析的常用方法
    - ✧ 惟密文攻击法 (Cipher Text only Attack)
      - ◌ 密码分析者知道一些消息的密文，试图恢复尽可能多的消息明文，并且试图推算出消息的加密密钥。
    - ✧ 已知明文攻击 (Known Plain Text Attack)
      - ◌ 密码分析者不仅知道一些消息的密文，而且知道与这些密文对应的明文，试图推算出消息的加密密钥和算法。

2.1 Cryptology Introduction

2.1.1 Introduction

- **密码分析**
  - 密码分析的常用方法
    - ✧ 选择明文攻击 (Chosen Plain Text Attack)
      - ◌ 密码分析者不仅知道一些消息的密文以及与之对应的明文，而且可以选择被加密的明文 (这种选择可能导致产生更多的关于密钥的信息)，试图推算出消息的加密密钥和算法。
      - ◌ 例如：攻击者获得对加密机的暂时访问， 因此他能选择明文串 *x* 并通过加密机得到相应的密文串 *y*。
    - ✧ 选择密文攻击 (Chosen Cipher Text Attack)
      - ◌ 密码分析者能够选择不同的密文并且得到相应的，试图推算出消息的加密密钥。
      - ◌ 例如：攻击者获得对解密机的暂时访问， 因此他能选择密文串 y 并通过解密机得到相应的明文串 *x*。

2.1 Cryptology Introduction

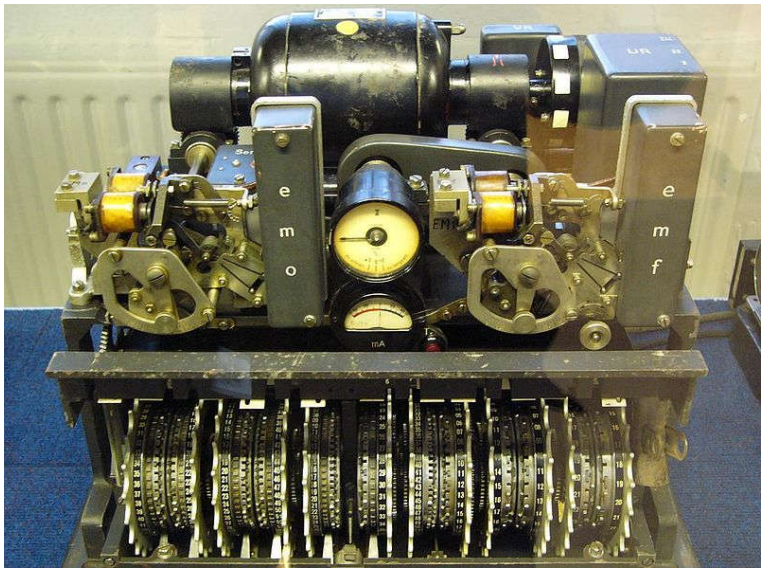
2.1.1 Introduction

- **密码分析**
  - 密码分析的其他方法
    - ✧ 旁路攻击 (Side Channel Attack)
      - ◌ 密码分析者通过收集外部信息 (例如能量消耗检测、辐射检测等) 来破解密码。
    - ✧ 重放攻击 (Replay Attack)
      - ◌ 攻击者捕获一些类型的数据，通过再次提交数据欺骗接收方的认证过程。
    - ✧ 统计攻击
      - ◌ 密码分析者对截获的秘闻进行统计分析，将结果和明文的一些已知统计规律做对照，从中提取明文和密文之间可能的变换信息。

2.1 Cryptology Introduction

2.1.2 History

- **The Manual Era**
- **The Mechanical Era**
- **The Modern Era**



German Lorenz cipher machine, used in World War II to encrypt very-high-level general staff messages

2.1 Cryptology Introduction

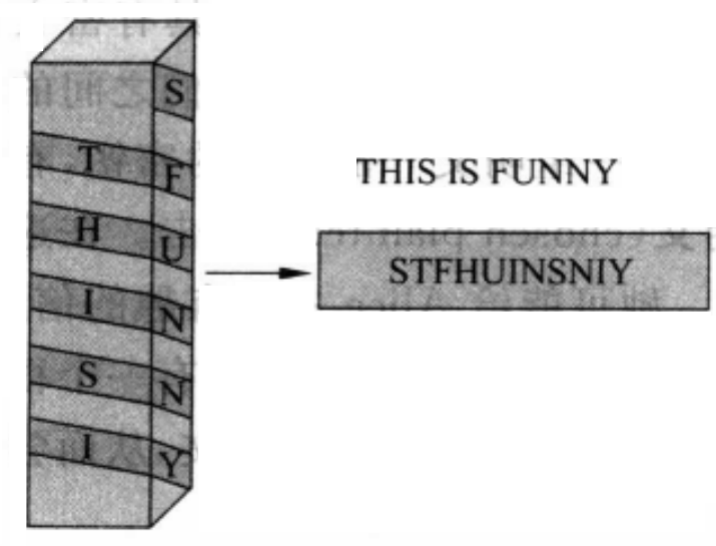
2.1.2 History

- 人工阶段
  - 记载表明，许多古代文明，包括埃及人、希伯来人、亚述人都在实践中逐步发明了密码系统。
  - 从某种意义上说，战争是科学技术进步的催化剂。人类自从有了战争，就面临着通信安全的需求。
  - 古代加密方法大约起源于公元前440年的古希腊战争。当时为了安全传送军事情报，奴隶主剃光奴隶的头发，将情报写在奴隶的光头上，待头发生长后将奴隶送到另一个部落，再次剃光头发，原有的信息复现出来，从而实现这两个部落之间的秘密通信。

2.1 Cryptology Introduction

2.1.2 History

- 人工阶段
  - 塞塔式密码
    - ✧ 公元前400年，斯巴达人就发明了“塞塔密码”(scytail/skytale)，即把长条纸螺旋形斜绕在一个多棱棒上，然后沿着棍子纵轴的方向书写文字。解下来后，纸条上的文字消息杂乱无章、无法理解，这就是密文，但将它绕在另一个同等尺寸的棒子上后，就能看到原始的消息。



2.1 Cryptology Introduction

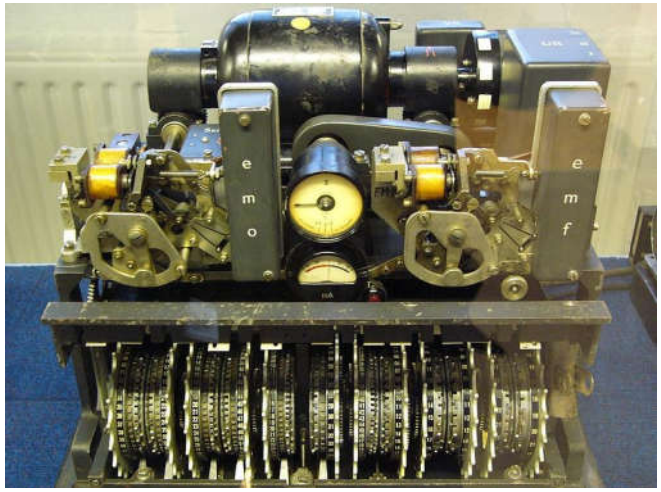
2.1.2 History

- 人工阶段
  - 我国古代也早有以藏头诗、藏尾诗、漏格诗及绘画等形式，将要表达的真正意思或“密语”隐藏在诗文或画卷中特定位置的记载，一般人只注意诗或画的表面意境，而不会去注意或很难发现隐藏其中的“话外之音”。

2.1 Cryptology Introduction

2.1.2 History

- **机械阶段**
  - 古典密码的加密方法一般是文字置换，使用手工或机械变换的方式实现。古典密码系统已经初步体现出近代密码系统的雏形，它比古代加密方法复杂，其变化较小。古典密码的代表密码体制主要有：单表代替密码、多表代替密码及转轮密码。



2.1 Cryptology Introduction

2.1.2 History

- 现代阶段
  - 密码学在20世纪70年代形成一门新的学科，这是受计算机科学蓬勃发展的刺激和推动的结果。快速电子计算机和现代数学方法一方面为加密技术提供了新的概念和工具，给密码设计者带来了前所未有的自由，另一方面也给破译者提供了有力武器。

2.1 Cryptology Introduction

2.1.2 History

- **古典密码阶段**
  - 古代 – 19世纪末
- **近代密码阶段**
  - 20世纪初 - 1949
- **现代密码阶段**
  - 1949 Claude Shannon “The Communication Theory of Secrete System”
- **公钥密码阶段**
  - 1976, W. Diffie, M. Hellman “New Directions in Cryptography”

2.1 Cryptology Introduction

2.1.2 History

- 古典密码阶段
  - 古典密码体制的安全性在于保持算法本身的保密性，受到算法的限制。
    - ✧ 不适合大规模生产
    - ✧ 不适合规模较大或者人员变动较大的组织使用
    - ✧ 用户被动选择，无法了解算法的安全性
  - 古典密码的种类
    - ✧ 替代密码 (Substitution Cipher)
      - ◌ 单字母代替 (Stream Cipher)
      - ◌ 多字母代替 (Block Cipher)
    - ✧ 换位密码 (Transposition Cipher)
    - ✧ 前两者的组合

2.1 Cryptology Introduction

2.1.2 History

- 近代密码阶段
  - 近代密码阶段的标志是机械密码/机电密码，用机电设备代替人工进行加密和解密操作。
    - ✧ 典型的 Rotor Machine 轮转密码机
  - OTP (One-time Pad) 一次一密乱码本
    - ✧ Major J. Mauborgne, Gilbert Vernam (AT&T), 1917
      - ◌ 不重复使用乱码本
      - ◌ 使用不可预知的随机数 (物理源) 构造乱码本
      - ◌ 理论上不可破解
    - ✧ 例：Secret => (18,5,3,17,5,19)
      + (15,8,1,12,19,5) = (7,3,14,3,24,24)
      => gmdcxx

2.1 Cryptology Introduction

2.1.2 History

- 近代密码阶段
  - Enigma
    - Arthur Scherbius, 1919
    - 4位 Egnima 机在二次大战期间装备德国海军
  - TYPEX
    - 英国打字密码机
      - 德国3位 Egnima 改进型
  - M-209
    - Boris Hagelin, 1934
    - 美国陆军使用

2.1 Cryptology Introduction

2.1.2 History

- 现代密码阶段
  - 1949 *Claude Shannon* “The Communication Theory of Secrete System”
  - 1967, *David Kahn* “The Codebreakers”
  - 1971-1973, IBM Watson Lab, *Horst Feistel*
  - 1974, LUCIFER algorithm (DES)
  - 新观点：数据的安全基于密钥而不是算法的保密

2.1 Cryptology Introduction

2.1.2 History

- 公钥密码阶段
  - 1976, *W. Diffie, M. Hellman* "New Directions in Cryptography"
  - 1977, *Rivest, Shamir* & *Adleman*, RSA Public Cryptography
  - 1990s, Elliptic Curve Cryptography
  - 公钥密码使得发端和收端的无密钥通信成为可能

2.1 Cryptology Introduction

2.1.2 History

- 公钥密码阶段
  - *Ronald L. Rivest* (1947 -), the Andrew and Erna Viterbi Professor of Computer Science at MIT's EECS.
    - ✧ *R. Rivest* is one of the inventors of the RSA algorithm (along with *Adi Shamir* and *Len Adleman* and shared with them the Turing Award in 2002). He is the inventor of the symmetric key encryption algorithms RC2, RC4, RC5, and co-inventor of RC6. He also authored the MD2, MD4, MD5 and MD6 cryptographic hash functions.

2.1 Cryptology Introduction

2.1.3 Concepts & Items

- Plain Text and Cipher Text
- Key and Key Space
- Cryptosystem Services
  - Confidentiality, Integrity, Authenticity, Non-repudiation, Access Control
- Cryptographic Methods
  - Symmetric, Asymmetric
- Attributes of Strong Encryption
  - Confusion, Diffusion

2.1 Cryptology Introduction

2.1.3 Concepts & Items

- Plain Text and Cipher Text
  - 明文 plain text
    - ✧ 信息以其最初的形式存在，被称为明文 (或 clear text)
  - 密文 cipher text
    - ✧ 被加密算法打乱之后的信息
- Key and Key Space
  - 密钥 key
    - ✧ 将明文转换为密文或者将密文转换为明文的算法中使用
  - 密钥空间 Key Space
    - ✧ 加密密钥的取值范围。通常以二进制位为单位，以位的数量来对独特密钥进行计数。密钥的位越长，其密钥空间也就越大。
      - ◌ 例如：当密钥长度为 r 时，密钥空间有 2^r 个元素

2.1 Cryptology Introduction

2.1.3 Concepts & Items

- Cryptosystem Services
  - Confidentiality 保密性原则
    - ✧ 只有发送人和授权接收人才能访问消息的内容
  - Integrity 完整性原则
    - ✧ 确保消息内容在发送方发出后和到达接收方之间不会发生改变，即保持一致性。
  - Authenticity 认证机制
    - ✧ 用于证明身份。认证过程保证对电子消息或文档来源的正确标示。
  - Non-repudiation 不可抵赖原则
    - ✧ 确保发送消息的用户不能对其发送消息的行为进行否认

2.1 Cryptology Introduction

2.1.3 Concepts & Items

- Cryptosystem Services
  - Access Control 访问控制
    - ✧ 确定谁能访问些什么内容
      - ◌ 例如数据库系统中对用户操作数据库记录权限的约束。
    - ✧ 访问控制矩阵和访问控制表 (ACL) 是常见的数据结构
    - ✧ 访问控制与两大领域相关：角色管理和规则管理
      - ◌ 角色管理考虑对用户方的控制
      - ◌ 规则管理考虑对资源方的控制

2.1 Cryptology Introduction

2.1.3 Concepts & Items

- Cryptosystem Services
  - Symmetric Cryptography 对称加密
    - ✧ 应用较早、技术比较成熟的加密算法。
    - ✧ 在对称加密系统中，数据发信方将明文 (原始数据) 和加密密钥一起经过对称加密算法处理后，转换成密文发送出去。收信方收到密文后，需要使用加密时所使用的密钥以及相同加密算法的逆算法对密文进行处理，才能使其恢复成可理解的明文。
    - ✧ 对称加密算法中使用的密钥只有一个，发收信双方都使用这个密钥对数据进行加密和解密，这就要求解密方事先必须知道加密密钥。(Ref. to Sec.2.2)

2.1 Cryptology Introduction

2.1.3 Concepts & Items

- Cryptosystem Services
  - Asymmetric Cryptography 非对称加密
    - ✧ 与对称加密不同，非对称加密需要两个密钥：公开密钥 (public-key) 和私有密钥 (private-key)。公开密钥与私有密钥一一配对，如果用一个公开密钥对数据进行加密，则只有用其对应的私有密钥才能实施解密；如果用一个私有密钥对数据进行加密，也只有用其对应的公开密钥才能解密。
    - ✧ 加密和解密使用的是两个不同的密钥，所以这种算法被称为非对称加密算法。 (Ref. to Sec.2.3)

2.1 Cryptology Introduction

2.1.3 Concepts & Items

- Attributes of Strong Encryption (*Shannon's* Condition)
  - Confusion 模糊性
    - ✧ 隐藏所有的局部模式，让密文与密钥之间的统计关系尽量复杂，敌手即使获取了关于密文的一些统计特性，也无法推测密钥。使用更为复杂的非线性替换，可能得到理想的混淆效果。
  - Diffusion 扩散性
    - ✧ 让明文中的每一位影响密文中的多位，或者说让密文中的每一位受明文中的多位的影响，从而更好地隐蔽明文的统计特性。理想的扩散是让明文中的每一位影响密文中的所有位，或者说让密文中的每一位受明文中所有位的影响。
    - ✧ 乘积和迭代有助于实现扩散和混淆。选择某些较简单的受密钥控制的密码变换，通过乘积和迭代可以取得比较好的扩散和混淆的效果

2.1 Cryptology Introduction

2.1.4 Different Types of Cryptosystem

- 密码体制
  - 它是一个五元组 (P, C, K, E, D)，满足条件：
    - (1) P 是可能明文的有限集；(明文空间)
    - (2) C 是可能密文的有限集；(密文空间)
    - (3) K 是一切可能密钥构成的有限集；(密钥空间)
    - (4) 任意 $k \in K$，有一个加密算法 $e_k \in E$ 和相应的解密算法 $d_k \in D$，使得 e_k 和 d_k 分别为加密解密函数，满足 $d_k(e_k(x))=x$，这里 $x \in P$。

2.1 Cryptology Introduction

2.1.4 Different Types of Cryptosystem

- Restricted & Key-based Cipher
  - 受限制的算法
    - ✧ 算法的保密性基于保持算法的秘密
  - 基于密钥的算法
    - ✧ 算法的保密性基于对密钥的保密

2.1 Cryptology Introduction

2.1.4 Different Types of Cryptosystem

- Symmetric & Asymmetric Cipher
  - 对称密码体系
    - ✧ 又称传统密码算法、单密钥算法、秘密密钥算法。
    - ✧ 对称密码体制的加密密钥和解密密钥相同，或实质上等同 (从一个易于推出另一个)。
    - ✧ 例如：DES, 3DES, IDEA, AES
- Symmetric & Asymmetric Cipher
  - 非对称密码体系
    - ✧ 又称公钥密码算法 (Public-key Cipher)。
    - ✧ 非对称密码体制的加密密钥和解密密钥不同，而且从一个很难推出另一个。其中的加密密钥可以公开，称为公钥 (Public key)；解密密钥必须保密，称为私钥 (Private key)。
    - ✧ 例如：RSA, ECC, ElgGmal

2.1 Cryptology Introduction

2.1.4 Different Types of Cryptosystem

- Block & Stream Cipher
  - 分组密码
    - ✧ 将明文分成固定长度的分组块，用相同密钥和算法对每一块进行加密，输出也是固定长度的密文分组。
    - ✧ 例如：DES, IDEA, RC2, RC4, RC5
  - 流密码
    - ✧ 又称序列密码。
    - ✧ 流密码每次只加密位或一个字节的明文。
    - ✧ 例如：OTP, Vernam

2.1 Cryptology Introduction

2.1.4 Different Types of Cryptosystem

- Substitution & Permutation Cipher
  - 替换密码
    - ✧ 明文中的每一个字符被替换成密文中的一个字符，接收者对密文字符做反向替换就可以恢复明文。
  - 置换密码
    - ✧ 又称换位密码 (Transposition Cipher)。
    - ✧ 置换算法将明文的字符打乱，得到密文。

2.1 Cryptology Introduction

2.1.5 Management of Cipher Keys

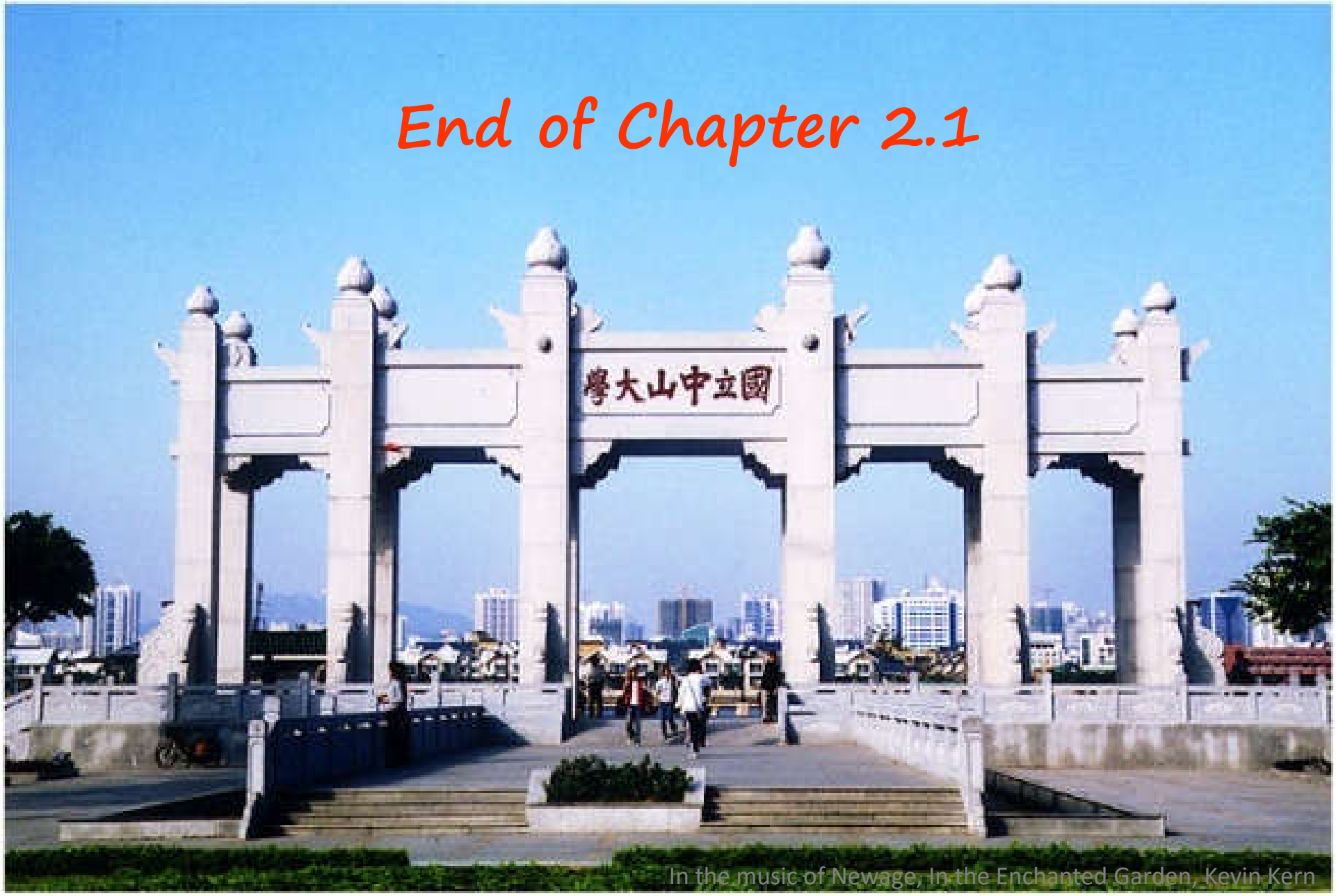
- 密钥管理的概念
  - 密钥管理的重要性
    - ✧ 密钥是密码体系的中心要素
    - ✧ 密钥管理是安全性保障的关键点
  - 密钥管理的安全策略
    - ✧ 密钥的产生、存储、分配、删除、归档等管理行为必须符合一个既定的安全策略。
  - 密钥管理的内容
    - ✧ 密钥管理覆盖密钥从产生到销毁的整个生命周期，包括系统初始化、密钥的产生、存储、备份/恢复、装入、分配、保护、更新、泄露处置、撤销、销毁等内容。
    - ✧ 密钥管理需要确定密钥生存周期策略。

2.1 Cryptology Introduction

2.1.5 Management of Cipher Keys

- 密钥管理的概念
  - 密钥的产生
    - ✧ 密钥的长度
    - ✧ 密钥的类型
    - ✧ 密钥的产生方式
      - ◌ 集中式
      - ◌ 分散式
  - 密钥的分配
    - ✧ 无中心的密钥分配
    - ✧ 中心化的密钥分配
      - ◌ KDC 的支持
    - ✧ 公钥体制的密钥分配

End of Chapter 2.1



In the music of Newage, In the Enchanted Garden, Kevin Kern