下发solution后看那几页？？

P28-32

P33

1. 密码学、加密学、密码分析学等 P5

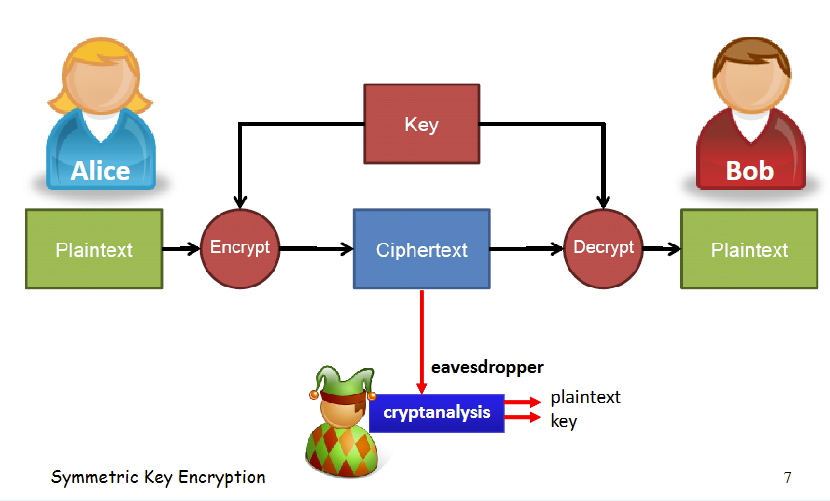
- Cryptology 密码学（加密和解密）

- Cryptograhy 加密学 entryption

- Crypt**analysis** 密码分析学（解密） detryption

- Crypto 加密解密+不可否认性、身份验证等等，更近似于信息安全的定义了。

2.对称加密术 Symmetric Cryptography P7



有**仨个比特串MCK**：Plaintext明文也叫Message，Ciphertext密文，Key密钥

有**两个算法ED**

E （entryption algorithm ）是 一个 从 K-Space 和 M - Space 到 C - Space 的方程

D （detryption algorithm）是一个 从 K - Space 和 C - Space 到 M - Space 的方程

****对称加密术其实就是加密秘钥和解密密钥是相同的加密方法****

Refer to :[你所能搜到的最全对称加密术讲解 - Symmetric Cryptography\_symmetriccrypto-CSDN博客](https://blog.csdn.net/qq_42141943/article/details/106039783)

3.Kerckhoffs Principle -----No “security through obscurity”

这一页PPT是想说对于Cryptanalysis 来讲我们已知什么，任务是什么——已知ED算法和密文C——懂得都懂了（故没有通过隐匿结构来实现安全性的说法），识别K并解出明文M（Plaintext）

接下来讲经典的对称加密术算法了

4.Caesar Cipher 凯撒密码 P9讲概念，P10-11讲一个实现例子，P12分析Caesar Cipher只有25个破解表太容易破解了，于是引入其他simple substitution ciphers，P13-18便是这个思路下的几个例子

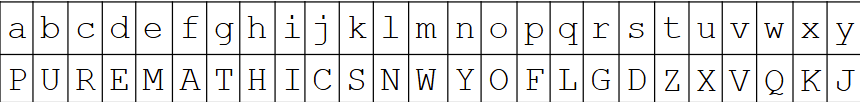
a type of substitution cipher

Key: n, the number of letters to shift

An example of P10-11

5.Simple substitution cipher

以一句格言为key，去除重复的字母（所以不会超过26个），生成对应的编码表（从a往z填，剩余没填满的自己再想办法匹配上比如剩余xyz位子和opq待填，按倒序填q-x,p-y,o-z）

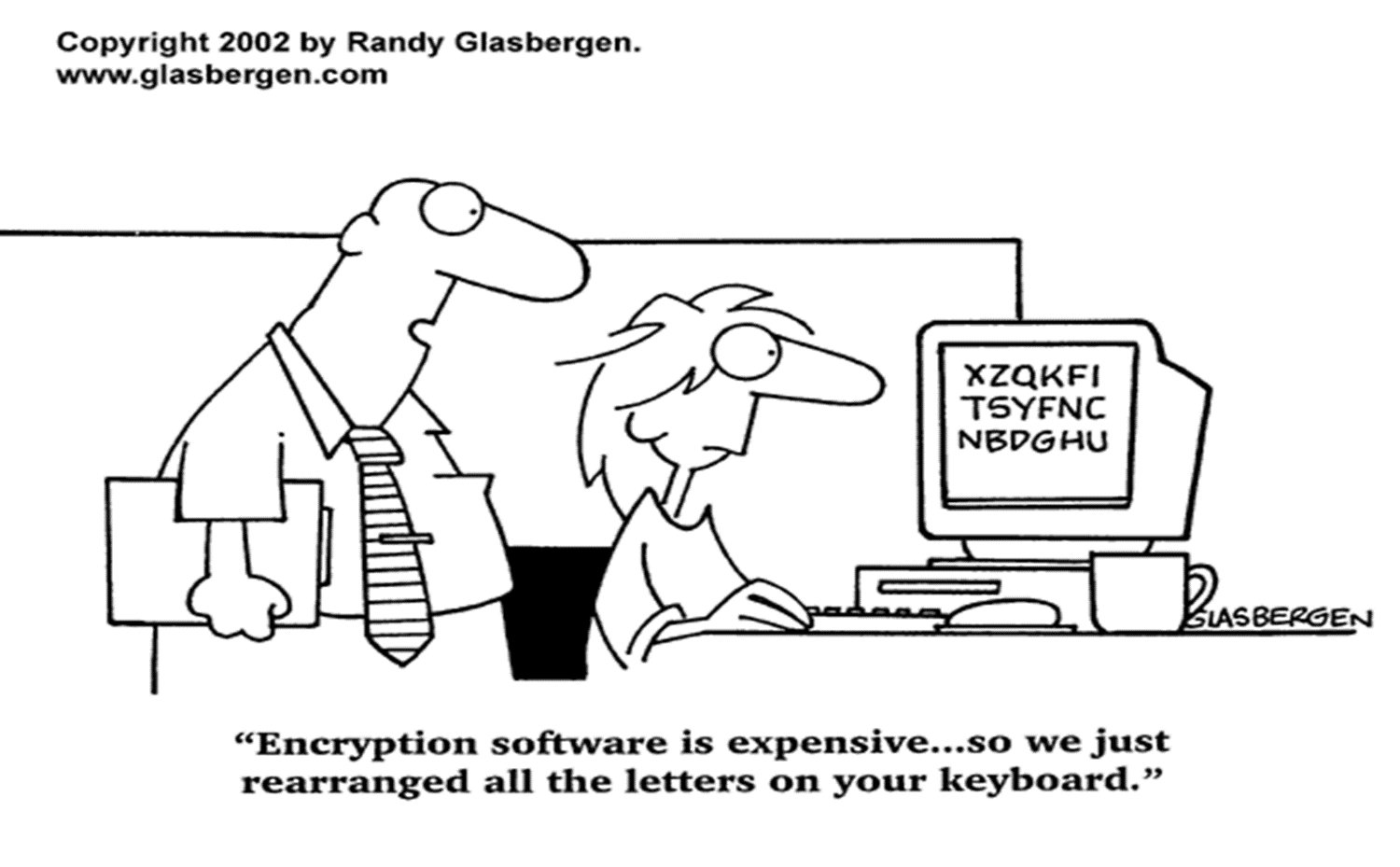


我怎么用这个表？上面小写字母的是明文M，下面大写字母的是密文C，加密时候根据上面转成下面，decrypt时候根据下面转成上面。

P13-15是一个例子：“pure mathematics is, in its way, the poetry of logical ideas”

P16又是一个例子：EIMBULJIWLNYANJMVLIURAHIWAI-->DEPARTMENTOFCOMPUTERSCIENCE

P17也算一个例子，或者说梗图，一语道破Simple substitution cipher的本质：



P18过渡先忽略。这的确是一个例子但没有给出secret key （alphabet），其实是属于接下来要讲的东西的一个引入过渡而已，但是PPT中没有注明这一点，所以第一次看和一周后再看这一页时想往前去找key alphabet根本找不到，也没有答案，但其实这是接下来词频分析的内容了。

接下来从Cryptanalysis角度来看Simple Substitution cypher了——

6.Simple Substitution Cipher的破解思路（暴力破解难度分析P20-21，引入词频分析P22-）

secret key--alphabet

Brute-force Attack 暴力破解，难度： 26！

引入Letter frequencies和**frequency analysis/**Statistical Attack的概念并举例一些语言学经验（linguistic knowledge ）P24-27

·Average letter frequencies in English (Beker and Piper, 1982) P24

·Pairs of letters in words are most likely to be: “ss”, “ee”, “tt”, “ff”, “ll”,

“mm” or “oo”.

· A one letter word is either “a” or “I”.

· Two letter words are commonly: “of”,“to”, “in”, “it”, “is”, “be”, “as”, “at”, “so”,“we”, “he”, “by”, “or”, “on” or “do”, in that order.

·Three letter words are commonly “the” or “and”.

·The letter h frequently goes before e (as in “he”, “the”, “then”, etc.) but

rarely goes after e. No other pair of letters has such an asymmetric relationship.

接下来几个连成一个例子P28-32：根据词频（但不是P24的，应该要有类似tutorial2中题目一样，说明已知在plaintext中a，e的词频最高才好，这个前文信息实在不足）、e前面常常是we、he等又猜一个词，再靠猜example（没错这就是**cribs**的技巧）又猜出几对，再依次判断这是key为6的Caesar Cipher

然后P33又是P18的例子了：

PBFPVYFBQXZTYFPBFEQJHDXXQVAPTPQJKTOYQWIPBVWLXTOXBTFXQWAXBVCXQWAXFQJVWLEQNTOZQGGQLFXQWAKVWLXQWAEBIPBFXFQVXGTVJVWLBTPQWAEBFPBFHCVLXBQUFEVWLXGDPEQVPQGVPPBFTIXPFHXZHVFAGFOTHFEFBQUFTDHZBQPOTHXTYFTODXQHFTDPTOGHFQPBQWAQJJTODXQHFOQPWTBDHHIXQVAPBFZQHCFWPFHPBFIPBQWKFABVYYDZBOTHPBQPQJTQOTOGHFQAPBFEQJHDXXQVAVXEBQPEFZBVFOJIWFFACFCCFHQWAUVWFLQHGFXVAFXQHFUFHILTTAVWAFFAWTEVOITDHFHFQAITIXPFHXAFQHEFZQWGFLVWPTOFFA

是有参考答案没错了，但是不晓得对不对以及这个过程！！要参考之后发的solution

回到Encoder的entryption或者说cryptography思路

7.如何beat/counter Frequency Analysis——**polyalphabetic substitution，Vigenère cipher维吉尼亚密码** 多字母替换

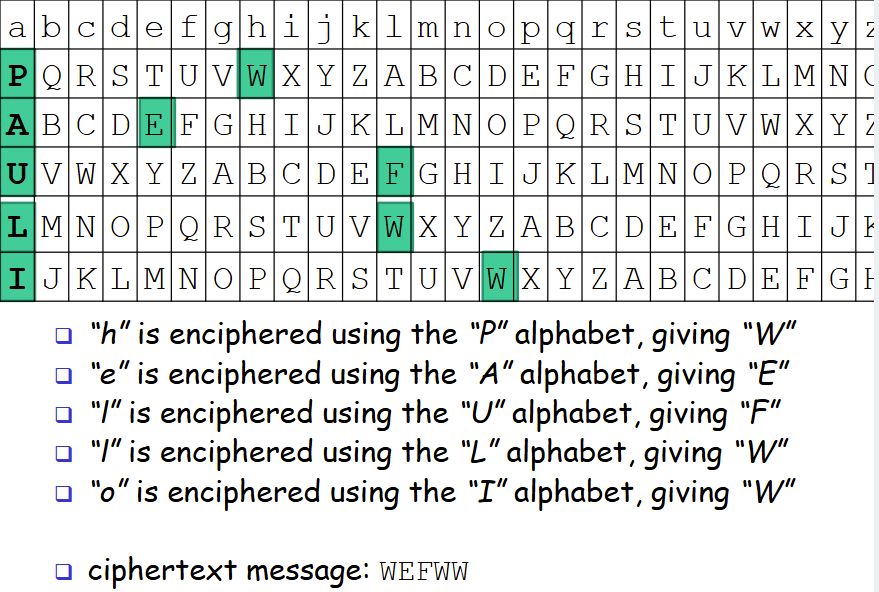
提及 P36

more than one cipher alphabet，enciphered in turn 多密码字母表，轮流来编码

interwoven Caesar cipher 该方法相当于交织型的凯撒密码

讲解概念，用一个例子说明 P37-41

hellobob >> paulipau



(a) enciphered the **two letters “l” to give different cipher letters “F” and “W”;**

(b) enciphered **different plaintext letters “h”, “l” and “o” to give the same ciphertext letter “W”**

300 years considered undecipherable (1553-1863)

同样的，又要准备回来decrypt角度了

1. Kasiski Examination method ——P44

1863 Kasiski Examination method卡西斯基检查法

猜key（前面例子是pauli）的长度——by最大公因数

如果发现ciphertext出现重复的词（间隔n），**大概率**plaintext中他们也是重复的 只不过经过了几个key长度后，由此key长度是间隔n的因数

如果发现多组cipher，那么这些间隔数n1n2的最大公因数**大概率**是key的长度

[密码学—Kasiski测试法Python程序-CSDN博客](https://blog.csdn.net/weixin_60521036/article/details/131278603)

9.Enigma Machine

多字母替換机器，你就想象是把键盘输入映射（前面那个meme图），每次解码时候都要把“键盘”调整成encrypt者一样的才行。

其他八卦的东西不用太管啦，反正也不考。

他这个问题是在于key长度太短，于是我们再次回到encryption角度，让

10.One-time Pad Encryption 一次性密码本加密 ——重点，要考的

Encryption: Plaintext Key = Ciphertext

Decryption: Ciphertext Key = Plaintext

eXclusive OR: 11=0; 10=1; 00=0

❑ Pad must be random, used only once

❑ Pad has the same size as message

Hello

Tutorial02

1、用了Caesar Cipher，但不晓得n=?

2、LFDPHLVDZLFRQTXHUHG，已知最高词频的plaintext字母是e和i

LFDPHVZRQTXUG

词频

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | L | F | D | P | H | V | Z | R | Q | T | X | U | G |
|  | 3 | 2 | 2 | 1 | 3 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |

所以e-L,i-H或者e-H,i-L，前者不符合Caesar Cipher，后者符合，n=3

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C |

so ‘L FDPH LVDZL FRQTX HUHG’ is I CAME IS AWI CONQUERED

I came is awi conquered??

I came I saw I conquered

1. Substitution Cipher
2. ecommerce-->EFYLLESFE
3. JKLLEPSTF-->symmetric
4. One-Time Pad
5. Stream Cipher

这俩我还真不懂，待会正好通过习题先了解一下

2. \*\*Teaching Materials\*\*

- 每周讲座幻灯片：提前几天在Canvas上发布，课后会附上额外评论。

- 教科书：William Stallings的《Cryptography and Network Security: Principles and Practices》（第3至8版）。

- 额外阅读和参考资料：核心工作在幻灯片中。

3. \*\*Weekly Teaching Pattern\*\*

- 讲座（2小时）：14:00-15:50，传统讲座，讨论设定阅读/案例研究。

- 辅导课（1小时）：16:00-16:50（AC5 416）或17:00-17:50（AC5 417），理论课程，纸质问题/练习，每周问题表。

- Canvas上的讨论：16:00-16:30/17:00-17:30开放讨论，16:30/17:30开始讨论辅导课解答。

4. \*\*Assessment\*\*

- 课程作业（40%）：2次家庭作业（各10%），分别在第6周和第13周提交。

- 中期测验（20%）：第7周（10月22日）进行。

- 期末考试（60%）：必须在期末考试中至少获得30%的分数。

5. \*\*Plagiarism\*\*

- 剽窃：不允许抄袭任何来源，必须正确引用/参考。

6. \*\*GenAI\*\*

- 编程任务或解决任何数值/逻辑问题时，学生不允许使用GenAI。

- 写作作业和报告中允许使用GenAI，但必须通过适当的引用和参考来确认其使用。

7. \*\*Intended Learning Outcomes\*\*

- 完成课程后，学生应能够：

1. 确定电子商务系统对数据保护的组织要求。

2. 展示对影响电子商务系统安全性的因素的知识。

3. 对电子商务系统的安全性进行批评和评估。

4. 描述管理电子交易、数据隐私保护和网络访问的相关法规。

5. 创建设计并分析保护电子商务系统和交易的安全机制。

8. \*\*Tentative Course Overview\*\*

- 第1周：行政和基本安全术语。

- 第2周：对称加密。

- 第4周：数论/非对称加密。

- 第5周：完整性。

- 第6周：认证（问题集1）。

- 第7周：中期测验。

- 第8-9周：密钥管理。

- 第10-12周：计算机安全和网络安全。

- 第13周：复习（问题集2）。

**9. \*\*Basic Security Goals (CIA)\*\***

**- 保密性（Confidentiality）：防止未经授权的信息披露。**

**- 完整性（Integrity）：防止未经授权的信息修改。**

**- 可用性（Availability）：防止未经授权的信息或资源扣留。**

**10. \*\*Threats\*\***

- 安全威胁：有deliberate和accidental，指可能破坏安全策略的手段，如数据泄露Exposure of data、篡改Tampering with data、拒绝服Denial of service。

**11. \*\*Adversaries\*\***

- 敌手：试图绕过安全措施的人，包括被动passive敌手（仅尝试获取未经授权的信息）和主动active敌手（采取更直接的行动，如未经授权的修改、删除、传输、伪造来源、未经授权的访问阻止）。

12. \*\*Security Services and Mechanisms\*\*

- 安全服务：应对威胁的措施，如提供保密性。

- 安全机制：提供服务的手段，如加密、数字签名。

13. \*\*Authentication\*\*

- 实体entity认证：在特定时间点验证声称的身份，通常用于连接开始时，解决伪装和重放威胁。

- 来源origin认证：验证数据的来源，不保护重放或延迟。

14. \*\*Access Control\*\*

- 访问控制：防止未经授权使用资源，包括通信资源、信息资源的读取、写入或删除、处理资源的执行。

**15. \*\*Non-repudiation\*\***

- 不可抵赖性：防止数据发送者否认发送数据（不可抵赖起源non-repudiation of origin），防止数据接收者否认接收数据（不可抵赖交付non-repudiation of delivery）。

16. \*\*Algorithms\*\*

- 算法：用于构建安全机制的方法，如加密算法（DES/3DES/AES、RSA/ECC）、MAC算法（CBC模式、HMAC）、数字签名算法（RSA、DSA、ECC）、哈希算法（SHA-3）、随机数生成算法（真随机或伪随机）。

17. \*\*Standards\*\*

- 标准：为特定活动和结果提供规则和指导的文件，旨在实现给定上下文中最大程度的秩序。

- 国际标准：如ISO、IEC、ITU。

- 北美标准：如IEEE、NIST、ANSI。

- 互联网标准：由IETF制定。

- 公司标准：如PKCS、SECG、PCI DSS。

这个提纲涵盖了电子商务信息安全课程的关键概念和术语，适合用于学习和复习。

引用自kimi.ai