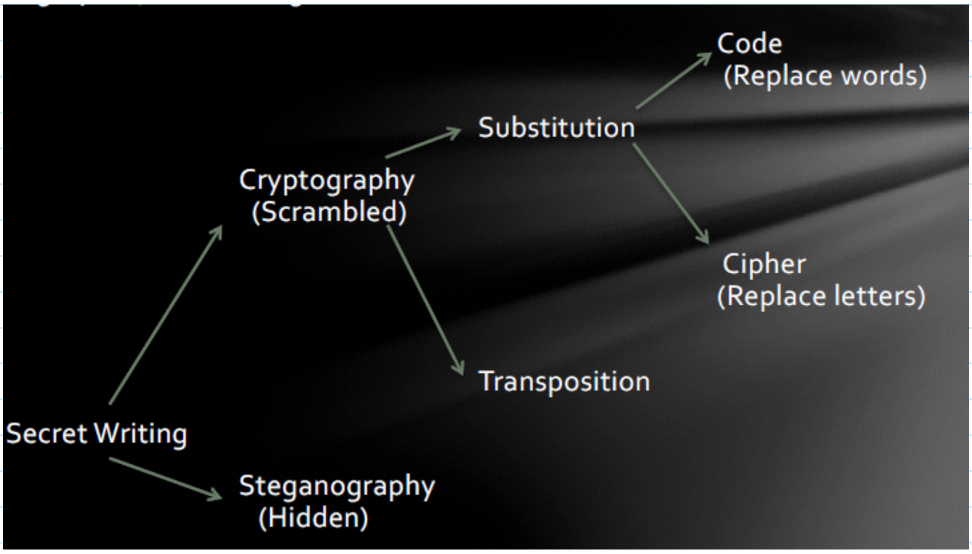
Chapter 2 Cryptography

2017年3月6日 11:24

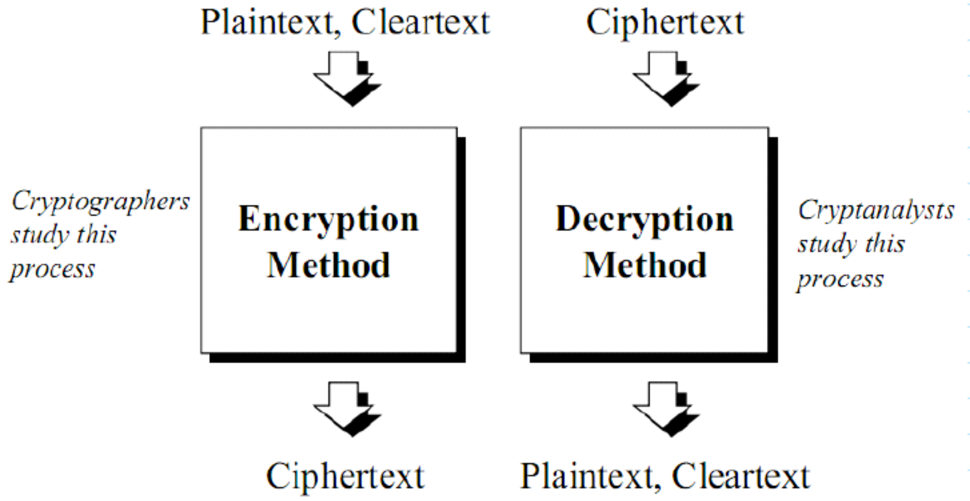
BY LSY

2017/3/8 8:13
Outlines:

- Fundamentals of Cryptography
- History of Cryptography
  - The Classical Age
  - ... Machine ...
  - ... Computer ...



Steganography：速记式加密 Cryptography：密码学



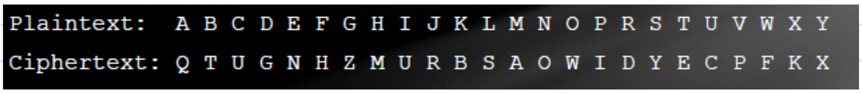
1.Terminology 术语

- Plaintext(plaintext，P)
- Ciphertext(ciphertext，C)
- Encryption(encryption method，E())
- Decryption(decryption method，D())
- Key（key，K)
- C = EK(P)

- P = DK(C)

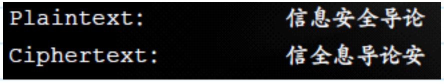
2.Algotirhm

- Substitution: 置换、替换



```
Plaintext:  A B C D E F G H I J K L M N O P R S T U V W X Y
Ciphertext: Q T U G N H Z M U R B S A O W I D Y E C P F K X
```

- Transposition: 位移



```
Plaintext:        信息安全导论
Ciphertext:       信全息导论安
```

3.Method of Attack/Analysis

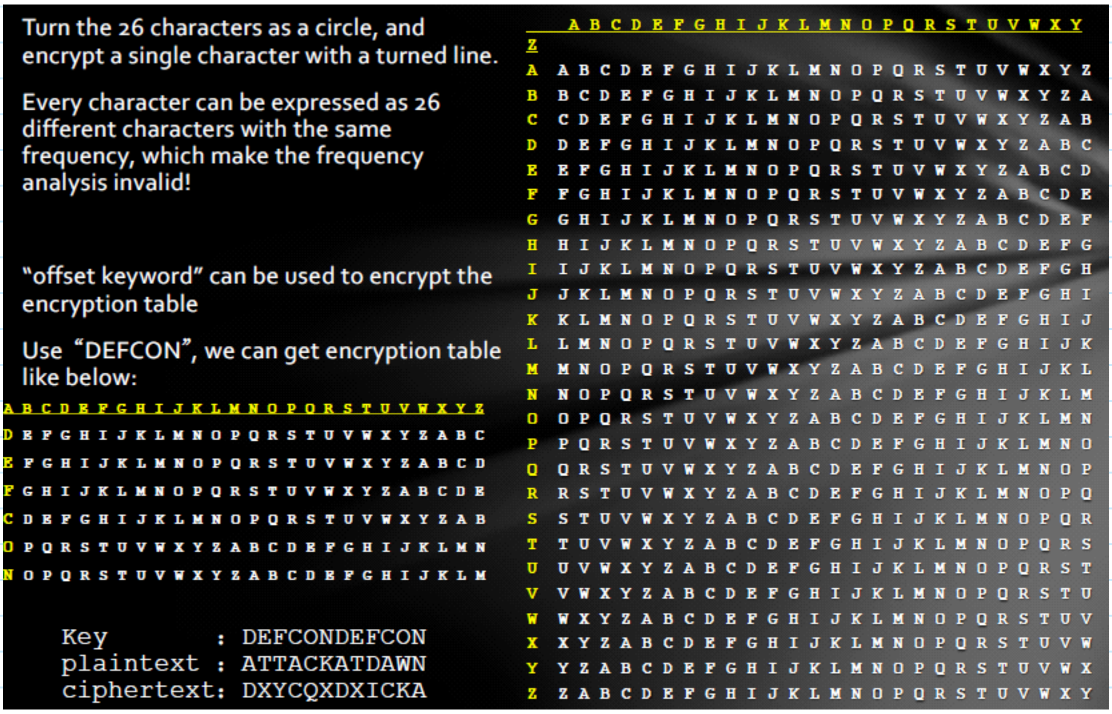
- Ciphertext-only: 只知道密文
- Known-plaintext: 知道一部分明文密文对
- Chosen-plaintest: choose some plaintext for target algorithm to encrypt to get the related ciphertext for attack
  选择明文攻击（预估一部分对应对，然后故意泄露进行验证）
- Chosen-ciphertext:choose some ciphertext for target algorithm to decrypt to get the related plaintext for attack
  选择密文攻击
- Related-key attack: choose some plaintext for the target to use two different key to encrypt to get the related ciphertext for attack

4. Result of Attack

- Total break: 完全被破解
- Global deduction: 发现算法
- Instance/Local deduction: 通过少量对应推广更广泛的
- Information deduction: Unknown Statistical information before about plaintext/ciphertext are found
- Distinguishing algorithm: 判断出是正常字符还是加密后的字符串

5. History of Cryptography

- Classic Ciphers
  - 棍子、腰带
  - 古希腊
  - 凯撒密码 Caesar Cipher
  - 玛丽女王
  - Frequency Analysis: 一一对应，因此统计规律对应
  - the Vigenère Square: Turn the 26 characters as a circle, and encrypt a single character with a turned line. 破除了统计规律



Turn the 26 characters as a circle, and encrypt a single character with a turned line.

Every character can be expressed as 26 different characters with the same frequency, which make the frequency analysis invalid!

“offset keyword” can be used to encrypt the encryption table

Use “DEFCON”, we can get encryption table like below:

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
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	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
C	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
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M

```
Key       : DEFCONDEFCON
plaintext : ATTACKATDAWN
ciphertext: DXYCQXDXICKA
```

	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
A	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
B	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	A
C	C	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
D	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
E	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	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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

  - The Kryptos Sculpture: 寻找可能重复的序列，然后找到密钥即循环的个数，再划分成相同加密方式的短文本
  - 豪密
- Machine Ciphers
  - Rotor Machine: Enigma
    - 符合Kerckhoffs's principle
    - Algorithm: whole machine + three rotors——invariable & hard to change
    - Key: initial setup + sequence of rotors + initial position of each rotor
    - Day Key + Message Key
    - 只改变初始化位置+连续发两遍

6. The reason of being cracked

- Misuse
- “Repetitions” leads to “Patterns”
- The “plug board arrangement” provides the most key spaces; however, it is weak to many attacks. Relatively speaking, the “initial setup of the rotors” is more secure in the “algorithm” layer --- it is broke by “Brute-force”

7. Way to crack encryption algorithm

- Search for “patterns”
- Reduce the “Complexity” / “Dimensions”
- Brute force
- Of course, you need strong “math-background” and a little “luck”

8. The third age of cryptography: computer ciphers