【InfoSec信息安全工程师】之【Crypto密码学】

1.开源，反而安全,但是并不代表所有关键信息都是开源，不加密的

2.Cypto:

（1）Crytology：密码学，更多的是一种科学，能够帮助我们去研究1）创造密码2）破解密码

（2）Cryptography:加密的学问

（3）Cryptanalysis:解密的学问

*学习一个科学，需要知道1）内涵2）外延

3.加解密的流程

（1）几个概念的补充1）plaintext:任何人都能读的2）ciphertext:只有特定的人能读

3)plaintext----encrypt---ciphertext----decrypt---plaintext

举例：假设这个世界上没有加解密理论，你怎么设计？

1bit：0，1

本质上就是一种Symmetric Key

A-----plaintext（I Love U）----encrypt（Key001）---ciphertext（akjfghmf……%￥……）----decrypt（Key001）---plaintext(I Love U)-----B

为了改进Symmetric Key的缺陷，我们引入的Asymmetric Key

A-----plaintext（I Love U）----encrypt（Key001）---ciphertext（akjfghmf……%￥……）----decrypt（Key002）---plaintext(I Love U)-----B