# 密码学复习资料

福光普照2020限定版

一、填空题

1.仿射密码y=ax+b(mod17)的密钥个数：\_\_\_\_\_\_\_\_\_

2.四种攻击方式：选择明文攻击、选择密文攻击、已知明文攻击、\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

3.唯一理想保密的密码体制是：\_\_\_\_\_\_\_

4.\_\_\_\_年RSA算法被提出

5.攻击的两大类：被动攻击、\_\_\_\_\_\_\_

6.密码学系统五元组(M,C,K,E,D)：\_\_\_\_\_\_\_\_

7.数据认证算法的功能是实现数据的\_\_\_\_\_\_\_\_性。

8.分组密码设计实现的两种方法：扩散和\_\_\_\_\_

9.IEEE802.11WLAN初期使用的加密算法为：\_\_\_\_\_

10.密码学发展的三个阶段：\_\_\_\_\_\_\_、近代密码学和现代密码学

二、名词解释

1. Diffie-Hellman密钥交换

2.中国剩余定理

三、计算题

1.已知消息是二进制的110000110101101111，背包序列为{62,93,81,88,102,37}，求密文

2.n=2，，用hill加密love

3.p=13，求离散对数值

4.利用Fermat计算

5.A5/1算法求前三个比特的值(考点大概就是这样，没来得及画图)

6.谈谈对密码学的认识