练习题部分参考答案

一、 填空题

1. 已知明文攻击

2. 主动攻击

3. 64

4. 160

5. CFB

6. 10110111

7. 1000

8. 列混合

9. 双向认证

10.数据加密密钥

11.密钥空间、解密算法

12.非对称密码体制

13.128bits

14.OFB CTR

15.同步序列密码

16.160 bits

17.$H(m) = s^e \bmod n$

18.会话密钥

19.已知明文攻击

20.E9

21.256

22.168

23.完整性、可用性

24.密码分组链接（CBC）、计数器（CTR）

25.对称

26.9

27.512

28.112

29.15

30.128bits、192 bits、256 bits

二、 填空题

1-5 TTTFT 6-10 FFTTF 11-15 FTTFT 16-20 FFTTT

21-25 TTFFT 26-30 FFTTF 31-35 TTFTF 36 F

三、 单选题

1-5 DADCB 6-10 BACAC 11-15 CDADA

16-20 CBCBA 21-25 BDCAD 26-30 CBDBC

31-32 AC