算法安全协议重点总结

Chapter 1

Nodes，links，and layers

Confidentiality integrity and authenticity

Trust model

Where is the original come from，安全性的基本来自于哪里，implicit

Thread model

Communication system security

Chapter 2

Feedback shift register sequences

Linear spans and BM Algorithm

Randomness criteria of a PRSG

Randomness properties of m-sequence

Nonlinear generators, BBS generators

Known attacks(相关性攻击)

Chapter 3

Design principles of stream ciphers

Stream ciphers in communication system

WG stream cipher(snow 3G)

Chapter 4

Design principles of block ciphers

DES, AES S-box

Encryption Modes

Hash Functions, MAC

Time-Memory Trade-Off attacks

Chapter 5

Security of public-key cryptography

DH key exchange

RSA, ECC(4Q)

Digital signature

Identity-based cryptography

Chapter 6

Infrastructure support

Authentication server, certificate authority

Key generation and distribution server

Signing server

Chapter 7 establish protected communications

Mutual authentication

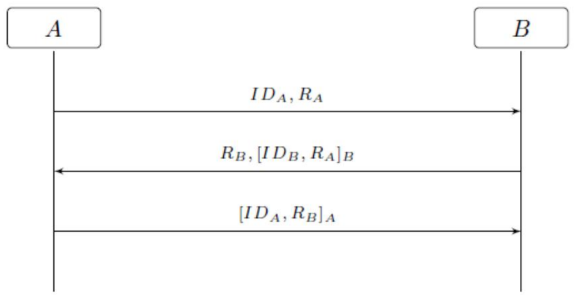
Key establishment
Cryptographic algorithm negotiation
Protected communications

Chapter 8
ISP SSH TLS

Homework 40%
Examination 60%
6.22 8 : 00 - 9 : 40 考试
6.21 16 : 00 - 17 : 40 答疑

Examination
True/False question, and give your reasons(4 * 5 = 20)
Basic problems (4 * 10)
Comprehensive problems (2 * 15)
Challenging problem(1 * 10)

2021 年算法协议和安全机制考试题
判断
1 sequence 0000 0001 的 linear span 是 8 吗，
2 f(x) = x^3 + x + 1 是 primitive polynomal（本元多项式）吗
3 linear 为 n 的序列周期最长是 2^n -1
4 m 序列满足 glomb 随机数判定规则吗
基础问题
1 f(x) = 1+x0+x1x2+x1x2x3 画出真值表和状态图 写出所有生成序列并说明周期长度。
2 序列 a13 = 1000 11111 0011 用 bm 算法求多项式，以及线性复杂度是多少
3 说出 diffHellman 协议的过程，和如何进行攻击
4 写出生日攻击计算方法，最少多少人能 50%同一天生日，以及用这个方法对 sha1 攻击的复杂度。
复杂问题
1 flaw 的[redacted] protrol 协议有什么 flaw，如何进行攻击，以及怎么提高安全性



Flawed mutual authentication Protocol 3

2 AES 的 s 盒，生成方法 M（一个矩阵）* [00] + [63]向量，

M = 1 0 0 0 1 1 1 1 × b0 + 1
1 1 0 0 0 1 1 1 b1 1
1 1 1 0 0 0 1 1 b2 0
1 1 1 1 0 0 0 1 b3 0
1 1 1 1 1 0 0 0 b4 0
0 1 1 1 1 1 0 0 b5 1
0 0 1 1 1 1 1 0 b6 1
0 0 0 1 1 1 1 1 b7 0

保证顺序 63 = 0110 0011

比如 00 变换后是 63

分别写出 [01] 和 [8D]经过 S 盒变换后的值是多少

挑战问题

1 判断下列生成序列的函数好不好，为什么，给你要怎么设计，x0 x1 x2（都是一个 SFR）

H1 = x0x1' + x1x2

H2 = x0 + x1 + x2

H3 = 取三者最大值，majority()

我的答案，都是自己考试写的，老师没给，仅供参考，错误地方以课本为准。

判断 1 2 3 4 都对

1 fx = x^8 +1 所有为 8

2 不能分解

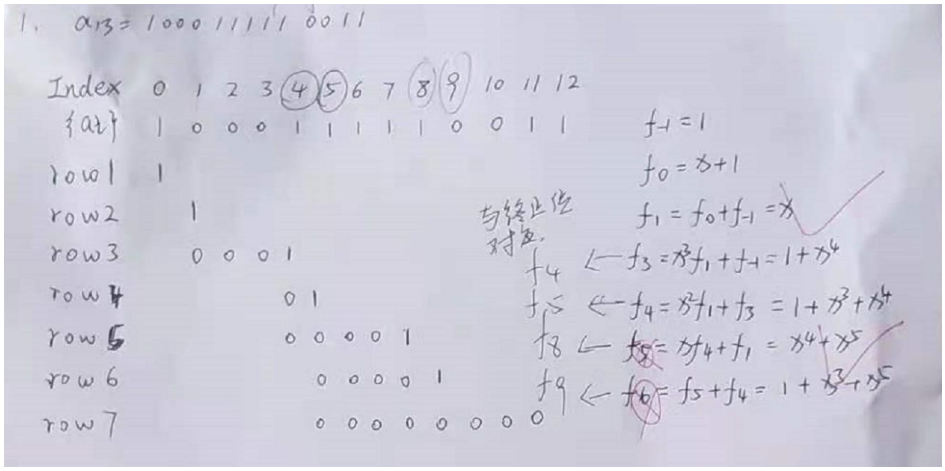
3 书上应该说了吧，我按直觉判断的

4 书上证明了 满足那三条性质

基础题

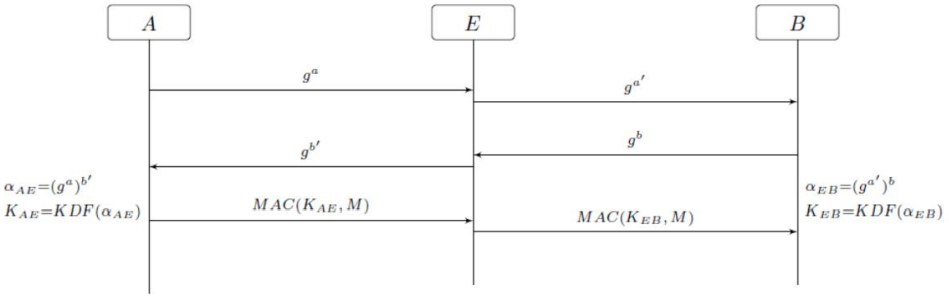
1 真值表直接写，状态图画出来是个 16◯，所以只有一种序列，周期是 16

2 和作业题一样，

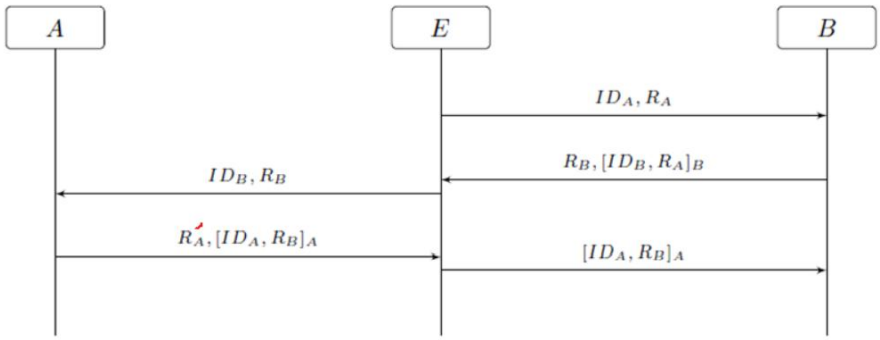


3 生日问题概率论讲过，书上写的 23 个人就行了，我正好记得这个，就直接写上去了，SHA1 160 比特，2^160 ,好像是开方，我这个没记清

4 dh 协议 Ya = g^Xa, Yb = g^Xb ， K = Ya^Xb = Yb^Xa = g^XaXb，这样，攻击方式，书上有，
a->e ga e->b ga’
B->e gb e->a gb’ 这样
攻击方法：

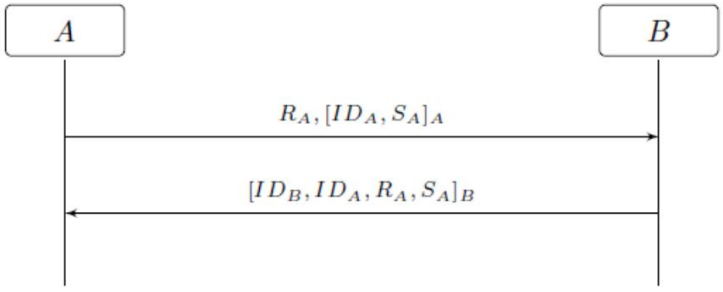


复杂题，
1 协议 flaw 缺点



Reflection attack

改进



Use a sequence number Protocol 2

2 AES
直接算
01 = 0000 0001 = b7b6b5b4b3b2b1b0 注意顺序
8D = 1000 1101
M = 1 0 0 0 1 1 1 1 × 1 + 1
1 1 0 0 0 1 1 1 0 1
1 1 1 0 0 0 1 1 0 0

1 1 1 1 0 0 0 1　　0　　0
1 1 1 1 1 0 0 0　　0　　0
0 1 1 1 1 1 0 0　　0　　1
0 0 1 1 1 1 1 0　　0　　1
0 0 0 1 1 1 1 1　　0　　0

= 1111 1000 + 1100 0110

= 0011 1110

然后换成十六进制倒过来 0111 1100，即为[7C]

M = 1 0 0 0 1 1 1 1 × 1 + 1
1 1 0 0 0 1 1 1　　0　　1
1 1 1 0 0 0 1 1　　1　　0
1 1 1 1 0 0 0 1　　1　　0
1 1 1 1 1 0 0 0　　0　　0
0 1 1 1 1 1 0 0　　0　　1
0 0 1 1 1 1 1 0　　0　　1
0 0 0 1 1 1 1 1　　1　　0

= 0010 1000 + 1100 0110

= 1110 1110

即为[77]

挑战问题

1 好不好

H1 好不好，不好，容易被相关性攻击，看课本的这个例子

Example 19 Let LFSRi, $i = 0, 1, 2$ have their respective characteristic polynomials $f_1(x) = x^2+x+1$, $f_2(x) = x^3 + x + 1$ and $f_3(x) = x^5 + x^3 + 1$. Those LFSRs generate m-sequences of period 3, 7, and 31 respectively. Let $\mathbf{a} = \{a_i\}$, $\mathbf{b} = \{b_i\}$ and $\mathbf{c} = \{c_i\}$ be the outputs of those three LFSRs, and

$$f(x_0, x_1, x_2) = x_0\bar{x}_1 + x_1x_2$$

$$\mathbf{s}^{40} = (s_0, \cdots, s_{39}) = (0100001110111010010110110011110110010111)$$

2 好不好，我觉得不好，设计的太简单了，但是输出结果的各种性质还是好的，0 和 1 的个数什么的

3 好不好，不好，有一个 1 全是 1，输出结果都是 1 了

怎么设计

我的看法，要达到 2 的效果，但不能过于简单，开放问题。