Homework 2: Your Name \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Chapter 3: (38pts)

3 (8pts)



5(8pts)

The key stream bits are 100000110…

this solution is for the original question which requires 32 bits output. So you can look at the first 8 bits only. Also depending on stepping first or generating key bit first, there could be one bit different from the standard solution , which are both fine. Please figure out the states of the three registers yourself.

14(8pts)

a. 64

b. 64

c. 56

d. 48

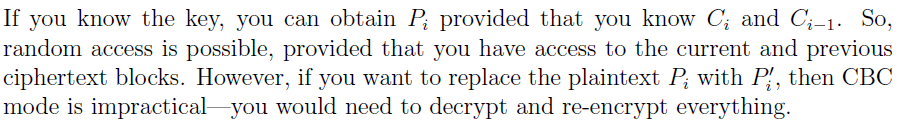
e. 16

f. 8

g. 6

h. 4

27(8pts)



In CTR mode, random access is easy as long as you know the count number for each block.

39.a(assuming k1!=k2) (6pts).

When decrypting, blocks 1 and 2 will be incorrect. Then when computing the

MAC we are re-encrypting with a different key, so the computed MAC will almost

certainly be different than the received MAC, and the tampering will be detected.

Chapter 4: (39pts)

2(9pts)

a. Nothing. It's a public key certificate, and public keys are public.

b. Hash the \message" and decrypt the signed quantity (using the CAs public key),

then compare the two.

c. Nothing. If Bob trusts the CA, he believes that the private key corresponding to

the public key in the certificate is held by Alice.

6(10pts)



12(10pts)

Encrypt the exchange with the shared key.

15 (5pts)

The private key is known only to the signer.

25(5pts)

No. Trudy has no way to determine the secret value gabt mod p that Alice and Bob

will share (short of solving a discrete log problem, that is).

Additional Questions:

1. (6) Consider a Diffie-Hellman scheme with a common prime *p=11* and a primitive root *g=2*.



1. If user A has a private key of 3, what is A’s public key?
2. If user B has a private key of 5, what is its public key?
3. What is their shared secret key K?

>>> Ya = 2^3 mod 11 = 8,

>>> Yb = 2^5 mod 11 = 10

>>> K = Ya^Xb mod 11 = 8 ^5 mod 11 = 10

1. (5 pts) Perform both encryption and decryption using the RSA algorithm for the following: p=3, q=13, e=5, and M=3. (you may guess d, you may use the repeated squaring based power reduction technique we introduced in the class)



**N = pq =39. Phi(n) = 2\*12 =24. ed =1 mod Phi (n) => 5d =1 mod 24 => d=5.**

**C = M^e mod n = 3^5 mod 39= 9.**

**M = C^d mod n = 9^5 mod 39 =3**

1. (6pts) Let h1 and h2 be two hash functions. Show that if either h1 or h2 is collision resistant, then the hash function h(x) = h1(x) ||h2(x), is collision resistant. (here ``||” means concatenation)

>>>Prove by contradiction: let us assume h1 is weak collision resistant (strong one is similar), it means that for a given x1 and h(x1), it is infeasible to find x2 != x1 such that h(x2) = h(x1). Now suppose h(x) = h1(x) ||h2(x) is not collision resistant. Then there exist x2 != x1, h(x2) = h(x1). That is, h1(x1) ||h2(x1) = h1(x2) ||h2(x2) => h1(x1) = h1(x2). This is a contradiction to our assumption.

1. (6 pts) What is a PKI? What are the three trust models for PKI (explain their meanings and example in some details)?

>>> refer to slides.