Homework 1. Due 5pm, May 1

Questions adopted from Ferguson, et al, *Cryptography Engineering*. One should not need to read Ferguson et al in order to answer these questions.

1. Key Exchange (adapted from *Cryptography Engineering*, Problem 2.3).

Consider a group of 30 people in a room who wish to be able to establish pair-wise secure communications in the future. How many keys need to be exchanged in total:

1.a. Using symmetric cryptography?

1.b. Using public key cryptography?

2. Key Strength and Brute Force Attacks (*Cryptography Engineering*, 3.8).

Suppose you have a processor that can perform a single DES encryption or decryption operation in 2^{-26} seconds, and a known plaintext-ciphertext pair encrypted under an unknown key. How many hours would it take, *on average*, to find that DES key, using an exhaustive approach:

2.a. With a single processor?

2.b. With a collection of 2^{14} processors?

4. Misusing Stream Ciphers, Part 1 (*Cryptography Engineering*, 4.3).

Suppose you, as an attacker, observe the following 32-byte ciphertext *C1* (in hex)

```
46 64 DC 06 97 BB FE 69 33 07 15 07 9B A6 C2 3D
2B 84 DE 4F 90 8D 7D 34 AA CE 96 8B 64 F3 DF 75
```

and the following 32-byte ciphertext *C2* (also in hex)

```
51 7E CC 05 C3 BD EA 3B 33 57 0E 1B D8 97 D5 30
7B D0 91 6B 8D 82 6B 35 B7 8B BB 8D 74 E2 C7 3B.
```

Suppose you know these ciphertexts were generated using CTR mode with the same nonce and the same key. (The nonce is implicit, so it is not included in the ciphertext.) You also know that the plaintext *P1* corresponding to *C1* is

```
43 72 79 70 74 6F 67 72 61 70 68 79 20 43 72 79
70 74 6F 67 72 61 70 68 79 20 43 72 79 70 74 6F.
```

What information, if any, can you infer about the plaintext *P2* corresponding to *C2*?

5. CBC Collisions (*Cryptography Engineering*, 4.6).

Let P_1, P_2 be a message that is two blocks long, and let Q_1 be a message that is one block long. Let C_0, C_1, C_2 be the encryption of the first plaintext using CBC mode with a random IV and a random key, and let D_0, D_1 be the encryption of Q_1 using CBC mode with a different, random IV and the same key. Suppose an attacker knows the first message P_1, P_2 and has intercepted both ciphertexts. Further suppose that, by random chance, $D_1 = C_2$. Show that the attacker can compute Q_1.

6. Hash Collisions (*Cryptography Engineering* 5.3).

Consider SHA-512-*n*, a hash function that runs SHA-512 and then outputs only the first *n* bits of the result. Write a program that uses a birthday attack to find and output a collision on SHA-512-*n*, where *n* is a multiple of 8 between 8 and 32. Your program may (*and probably should*) use an existing cryptography library. Time how long your program takes when *n* is 8, 16, 24, and 32, averaged over 5 (pseudo-randomized) runs for each *n*. Repeat each experiment three times, and report each time and the average time for each *n*. How long would you expect your program to take for SHA-512-256? For SHA-512-384? For SHA-512 itself? Include a copy of your program in your submission. (You are not being tested on the speed of your solution, though your program should complete within 120 minutes for *n*=32 – we have solutions that run in less than a second.)

7. CBC-MAC I (*Cryptography Engineering* 6.2).

Suppose *c* is one block long, *a* and *b* are strings that are a multiple of the block length, and $M_K(a \,||\, c) = M_K(b \,||\, c)$. Here, M_K is CBC-MAC with a random key *K*. Explain why the claim that $M_K(a \,||\, d) = M_K(b \,||\, d)$ for any message *d* is true. You may find it helpful to use one or more figures. Here || denotes string concatenation. Also, the equation is true regardless of the value of K; you do not know the key *K*.

8. CBC-MAC II (*Cryptography Engineering* 6.4).

Suppose message *a* is one block long and that you have received the MAC *t* for *a* using CBC-MAC under some random key unknown to the attacker. Explain how to forge the MAC for a particular two-block message of your choice. What is the two-block message that you chose? What is the tag that you chose? Why is your chosen tag a valid tag for your two-block message?

9. Stealing a Car Attack Tree (*Cryptography Engineering* 1.1).

Create an attack tree for stealing a car. For this and the other attack tree exercises, you can present your attack tree as a figure (like this figure http://www.schneier.com/paper-attacktrees-fig1.html from http://www.schneier.com/paper-attacktrees-ddj-ft.html; this figure was also presented in class), or you can present your attack tree as a list numbered in outline form (e.g., 1, 1.1, 1.2, 1.2.1, 1.2.2, 1.3, ...).

Your attack tree should be as complete as possible -- try not to overlook any branches. You must have at least one path of height four or greater (where the height includes the root and the leaf). You must also have at least two nodes with four or more children.

Sometimes attack trees can be very deep. In order to keep this problem tractable you can stop expanding on a path after the path from the root contains five nodes (including the root and the leaf); just add a note saying that this node can be expanded further. It is OK if some paths from the root are shorter.