ECE: Information and Network Security
Homework 4
Spring 2006

Chapter 8: Book Problems 3, 4

3. h can be computed quickly, so (1) is satisfied. However, $h(x\|0\|0\|\cdots) = x$, so it is not preimage resistant. Taking different numbers of 0-blocks yields collisions, so it is not strongly collision-free.

4. The probability that no two have birthdays in the same month is

$$\left(1 - \frac{1}{12}\right)\left(1 - \frac{2}{12}\right)\left(1 - \frac{3}{12}\right) = \frac{165}{288} \sim 0.573$$

Chapter 10: Book Problems 4, 5, 6

4. (a) Alice calculates $(\alpha^{yq})^x$ and Bob calculates $(\alpha^{xq})^y$. These are the same.

(b) Observe that the key is $(\alpha^q)^{xy}$. Since $\alpha^{Mq} = \alpha^{p-1} = 1$ there are only M possible values for α^{kq} for different values of k. Eve may find the key by calculating α^q and raising this to successive powers.

5. Suppose we arrange the participants in a ring, like Bob ¿ Ted ¿ Carol ¿ Alice ¿ Bob. Each person starts with α and raises it to their private exponent, e.g. Bob calculates α^b. They each send their respective result to the person to their right. The next round, they take what they received and raise it to their private exponent and pass it to their right. If we repeat this two more times, they will all have calculated α^{abcd}.

6. (a) Use $K = M_1 \oplus K_N$ and substitute $M_1 = M_2 \oplus K_H$ to get $K = M_2 \oplus K_H \oplus K_N$. Now substitute $M_2 = M_3 \oplus K_H$ and use the fact that $K_N \oplus K_N = 0$ to get $K = M_3 \oplus K_H$. (b) Observe that $K_N = M_3 \oplus M_2$ and $K = M_1 \oplus K_N$. Thus Eve can calculate the key.

Supplemental Problems:

1. Suppose Bob is a server, and Alice is a client. Bob is not allowed to store any challenges he issues to Alice (perhaps he is resource limited). To bypass this issue, the following protocol is proposed in which Alice sends back the challenge (nonce) to Bob:

$$A \to B : ID_A$$
$$B \to A : r$$
$$A \to B : \{r, E_{K_{AB}}(r)\}$$

where r is the nonce, and K_{AB} is a key shared between Alice and Bob. Does this protocol achieve mutual authentication? Is it secure?

Answer: No, it does not. It is possible for Eve (the eavesdropper) to replay Alice's messages at any time. Thus, since Bob does not store the challenges he sent, he can't check whether they were from a previous challenge or not. In essence, Bob needs to be able to remember his challenges in order to make this scheme work.

2. Consider the following authentication protocol. Alice generates a random message r and encrypts it with the key K she shares with Bob, and sends

$$A \to B : E_K(r)$$

to Bob. Bob deciphers it and adds 1 to r and sends

$$B \to A : E_K(r + 1)$$

to Alice. Alice deciphers and compares it with r. If the difference is 1, she knows that her correspondent shares the same key and is therefore Bob. If not, she assumes that her correspondent does not share K and so is not Bob. Does this protocol authenticate Bob to Alice? Why or why not?

Answer: Alice is able to compare r and "$r + 1$". Thus, she must be able to store r. It does provide authentication, as long as the r and K do not repeat. If Alice repeats an r for that K, then Eve will be able to see this repetition, and can replay the response. Hence, authenticity is provided so long as repetition is not going to happen. This requires extra storage on Alice's part.