CSCI 3403 **Erika Bailon**
Homework 3 **Fall 2018, CU-Boulder**

1. **Review 2.4** List three approaches to message authentication.

   (a) Message authentication code - involves the use of a secret key to generate small blocks of data that is appended to the message.

   (b) One-Way hash function - accepts a variable-size message M as input and produces a fixed-size message digest $H(M)$ as output.

   (c) Encryption - Although is not very safe

2. **Review 2.7** What properties must a hash function have to be useful for message authentication?

   (a) H can be applied to do a block of data of any size

   (b) H produces a fixed-length output.

   (c) $H(x)$ is relatively easy to compute for any given x, making both hardware and software implementations practical.

   (d) For any given code h, it is computationally infeasible to find x such that $H(x) = h$. A hash function with this property is referred to as **one-way** or **preimage resistant**.

   (e) For any given block x, it is computationally infeasible to find $y \neq x$ with $H(y) = H(x)$. A hash function with this property is referred to as **second preimage resistant**. This is sometimes referred to as **weak collision resistant**.

   (f) It is computational infeasible to find any pair (x, y) such that $H(x) = H(y)$. A hash function with this property is referred to as **strong collision resistant**.

3. **Review 2.9** List and briefly define three uses of a public-key cryptosystem?

   (a) Digital Signature
   Is a data-dependent bit pattern, generated by an agent as a function of a file, message, or other form of data block.

   (b) Symmetric key distribution
   It requires two parties to communicate securely with a share secret key.

   (c) Encryption of secret keys
   Using the same key to encrypt and decrypt data.

4. **Review 2.10** What is the difference between a private key and a secret key?

   As I mentioned in the previous question, a secret key is the one used for symmetric cryptography, meaning same key to encrypt and decrypt. This means that the two people who are sending/receiving messages to/from each other, have the same key, and is secret, and therefore no one else knows it.
   In the contrary, the private key is the one used for asymmetric cryptography. This key is only used by one end of the communication. Its usually used with a public key too.

5. **Problem 2.4**. Perhaps the simplest "serious" symmetric block encryption algorithms is the Tiny Encryption Algorithms (TEA). TEA operates on 64-bit blocks of plaintext using a 128-bit key. The plaintext is divided into two 32-bit blocks (L_0, R_0), and the key is divided into four 32-bit blocks (K_0, K_1, K_2, K_3). Encryptions involves repeated application of a pair of rounds, defined as follows for rounds i and $i+1$:

$$\begin{gathered} L_i = R_{i-1} \\ R_i = L_{i-1} \boxplus F(R_{i-1}, K_0, K_1, \delta_i) \\ L_{i-1} = R_i \\ R_{i-1} = L_i \boxplus F(R_i, K_2, K_3, \delta_{i+1}) \end{gathered}$$

   where F is defined as

$$F(M, K_j, K_k, \delta_i) = ((M \ll 4) \boxplus K_j) \oplus ((M \gg 5) \boxplus K_k) \oplus (M + \delta_i)$$

   and where the logical shift of x by y is detonated by $x \ll y$; the logical right shift x by y is denoted by $x \gg y$; and δ_i is a sequence of predetermined constants.

   (a) Comment on the significance and benefit of using the sequence of constants
   Using it is beneficial because you are changing the cypher text producing a 128 bit key every pair of rounds and the constant that is changing, acts as another key.

   (b) Illustrate the operation of TEA using a block diagram or flow chart type of depiction
   **Please see page attached written by hand - SORRY

   (c) If only one pair of rounds is used, the the cyphertext consists of the 64-bit block (L_2, R_2). For this case, express the decryption algorithm in terms of equations.
   **Please see page attached written by hand - SORRY

(d) Repeat part (c) using an illustration similar to that used for part (b)
**Please see page attached written by hand - SORRY

6. **Problem 2.5**. In this problem, we will compare the security services that are provided by digital signatures (DS) and message authentication code (MAC). We assume Oscar is able to observe all messages sent from Alice to Bob and vice versa. Oscar has no knowledge of any keys but the public one in case of DS. State whether and how (*i*) DS and (*ii*) MAC protect against each attack. The value auth(x) is computed with a DS or a MAC algorithm, respectively.

   (a) (Message integrity) - *i*) - Bob will be able to tell because of the signature verification algorithm
   ii) - Bob will be able to tell because the calculations of the code will differ from the record code.

   (b) (Replay) - *i*) - Bob won't be able to tell if Oscar hack it because the code was not modify and the key is also not modified.
   ii) - Same, Bob won't be able to tell because there won't be changes only 100 messages with the same text.

   (c) (Sender authentication with cheating third party) - *i*) - Bob will be able to tell that Oscar didn't send the message because Oscar doesn't have a key so he can't encrypt a message without a key, no hash function that will give a valid verification.
   ii) Bob will be able to tell that Oscar didn't send it because Oscar doesn't have a key so there won't be a key to compare.

   (d) (Authentication with Bob cheating) - *i*) - Yes, Alice can hash the message to prove whether or not her key is in there, since Bob doesn't have her key, it'll be easy to prove it wasn't sent by her.
   ii) - Alice won't be able to prove she didn't send it since they both share the same key and Bob could've encrypted the message with the key and say it was Alice.

7. **Problem 2.6**. Suppose H(m) is a collision-resistant hash function that maps a message of arbitrary bit length into an n-bit hash value. Is it true that, for all messages $x, x^{'}$ with $x \neq x^{'}$, we have $H(x) \neq H(x^{'})$? Explain your answer.

   It is computationally infeasible, therefore is FALSE. We have an arbitrary number of inputs and according to what we saw in clase, if we get to a point where the hash values are greater than 2^{512} then it is impossible. We MUST have for sure some values hashing to the same function.

8. **Problem 2 FROM HOMEWORK 2** The following cipher text was produced by the Caeser cipher: **qeb mxpptloa fp nnwwnnw**

   **Please see page attached - Sorry I didn't type it either