Homework #3

Out : September 23, 4:30 pm 1997
Due : September 30, 12:30 pm 1997

1. Imagine you are Eve, and you wake up one morning and learn that a message was sent from Alice to Bob in which one digit was encrypted by adding (mod 10) a randomly selected key to the cleartext.

   (a) As far as you know at this point, what are the possible cleartexts?

   (b) Imagine that an hour later, you learn the cyphertext. Now what are the cleartexts consistent with what you know?

   (c) Now say you wake up the following day, and learn that Bob has sent a message to Alice in which TWO digits were encrypted by randomly choosing a key and adding it to each of the digits (mod 10). Based on what you know, what are the possible cleartexts?

   (d) Once again, after pondering this for an hour, you observe the cyphertext itself. Now what are the cleartexts consistent with what you know?

   For each of the encryption functions described in problems 2-7 below, answer the following questions.

   (i) Is the function uniquely decryptable for every key? If so, define the decryption function using a rule. If not, give a key and two cleartexts that map to the same cyphertext.

   (ii) Is the function uniquely de-keyable for every cleartext? If so, show that for every cleartext the function mapping the key to the cyphertext is invertible (by giving the rule for the inverse). If not, give a cleartext and two keys that map to the same cyphertext.

   (iii) If part ii showed that the encryption function was not uniquely de-keyable, is it nevertheless perfectly secure? If so, sketch a probability distribution for the cyphertext, assuming uniformly random selection of keys. Be sure to label the vertical axis to show what the probability values are. If not, provide two different cleartexts for which the distribution of cyphertexts are different.

   Example:

   - *Rule:* $encrypt(clear, key) = clear + key \pmod{10}$
   - *Cleartext space: integers 0 through 9*
   - *Key space: integers 0 through 9*
   - *Cyphertext space: integers 0 through 9*

   (i) Yes, this function is uniquely decryptable for every key. The rule for the decryption function is $decrypt(cyph, key) = cyph - key \pmod{10}$.

   (ii) Yes, this function is uniquely de-keyable for every cleartext. The rule for the inverse is $key = cyph - clear \pmod{10}$.

(iii) The function is uniquely de-keyable, as demonstrated in part ii.

Example:

- *Rule:* $encrypt(clear, key) = clear * key \pmod{10}$
- *Cleartext space: integers 0 through 9*
- *Key space: integers 0 through 9*
- *Cyphertext space: integers 0 through 9*

(i) This function is not uniquely decryptable for every key. If the key is 5, for instance, the cleartexts 6 and 8 both encrypt to 0.

(ii) The function is also not perfectly de-keyable. If the cleartext is 2, the keys 3 and 8 both yield a cyphertext of 6.

(iii) The cleartexts 3 and 4 have different cyphertext distributions.

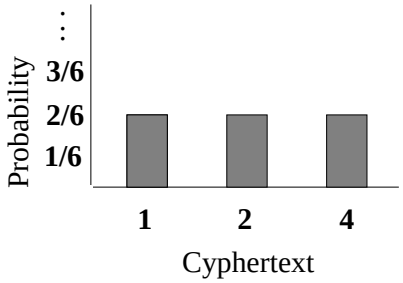
Example:

- *Rule:* $encrypt(clear, key) = (clear \cdot key^2)$ *rem* 7
- *Cleartext space: 1, 2, 4*
- *Key space: 1, 2, 3, 4, 5, 6*
- *Cyphertext space: 1, 2, 4*

(i) Yes, this function is uniquely decryptable for every key. The rule for the decryption function is $decrypt(cyph, key) = (\frac{cyph}{key^2})$ *rem* 7.

(ii) No, this function is not uniquely de-keyable. If the cleartext is 1, the keys 3 and 4 both yield cyphertexts of 2.

(iii) Despite the fact that this function is not uniquely de-keyable, it is perfectly secure. The probability distribution is uniform. Each possible cyphertext has a probability of $\frac{1}{3}$*:*



2. Rule: $encrypt(clear, key) = clear \cdot key$ rem 11
   Cleartext space: integers 1 through 10
   Key space: integers 1 through 10
   Cyphertext space: integers 1 through 10

3. Rule: $encrypt(clear, key) = clear^2 + key$ rem 13
   Cleartext space: integers 0 through 12
   Key space: integers 0 through 12
   Cyphertext space: integers 0 through 12

4. Rule: $encrypt(clear, key) = clear + key^2$ rem 7
   Cleartext space: integers 0 through 6
   Key space: integers 0 through 6
   Cyphertext space: integers 0 through 6

5. Rule: $encrypt(clear, key) = 4 \cdot clear + key^2$ rem 14
   Cleartext space: integers 0 through 13
   Key space: integers 0 through 13
   Cyphertext space: integers 0 through 13

6. Rule: $encrypt(clear, key) = (clear \cdot key^2)$ rem 5
   Cleartext space: 1, 4
   Key space: 1, 2, 3, 4
   Cyphertext space: 1, 4

7. Rule: $encrypt(clear, key) = clear + key$
   Cleartext space = 0, 1, 2, 3
   Key space = 0, 1, 2, 3
   Cyphertext space = 0, 1, 2, 3, 4, 5, 6

8. Make and provide us two multiplication tables, one with a modulus of 11 and the other with a modulus of 15. Using your tables, do the following operations. If the answer does not exist, say so and explain briefly.

   (a) $1/5 \pmod{11}$
   (b) $3/4 \pmod{15}$
   (c) $1/5 \pmod{15}$
   (d) $2/3 \pmod{11}$
   (e) $1/3 \pmod{15}$

9. In class, you saw the threshhold secret-sharing scheme: each person who is supposed to share the key gets a point on a line and the secret is the y-intercept of that line. Say we have divided up the key among several people, and you and one other person have gotten together to combine your keys. Your point is $x = 4$ and $y = 8$, and your partner's point is $x = 5$ and $y = 0$. The modulus is 11. What is the secret?

10. In this problem we address the use of a MAC (message authentication code). The modulus for this problem is 11. Alice and Bob have previously agreed upon a secret key consisting of the two mod-11 numbers a and b. Thus the MAC function is

$$f(x) = ax + b$$

so when Alice sends a message X, she should accompany the message with the MAC $f(X)$.

If Alice and Bob had been paying attention in class, they would know that the MAC is secure only if the key is used once. Unfortunately, they missed this fact, and they send two distinct messages with MACs derived using the same key (the same pair of numbers a and b). You, Eve, intercept these messages and MACs:

message: 4, MAC: 5
message: 1, MAC: 9

You decide to tamper with the second message, changing it to 3. What MAC should accompany this forged message to convince Bob that it is legitimate?