UEE4611 Assignment #9 Solution

1. Consider the following hash function. Messages are in the form of a sequence of numbers in $\mathbb{Z}_n, M = (a_1, a_2, ..., a_t)$. The hash value h is calculated as

$$\sum_{i=1}^{t} a_i^2 \mod n$$

for some predefined value n.

(a) Is this hash function collision resistant? Explain your answer.(10%)

(b) Calculate the hash value for $M = (189, 632, 900, 722, 349)$ and $n = 989$.(5%)

(a)

If $M = (a_1, a_2, a_3)$ and let $n = 2$.
It is easy to see when $M = (1, 1, 1)$ and $M = (2, 2, 1)$, their value of hash function is the same.
So the answer is No. This function is not collision resistant.

(b)

$h = (189^2 + 632^2 + 900^2 + 722^2 + 349^2) \equiv 229(\mod 989)$.

2. State the value of the padding field in SHA-512 if the length of the message is

(a) 2942 bits (5%)

(b) 2943 bits (5%)

(c) 2944 bits (5%)

(a)

$$2942 + x \equiv 896 (\mod 1024)$$
$$\rightarrow x = 2$$

We can know that it's two bits padding, so the answer is 10.

(b)

$$2943 + x \equiv 896 (\mod 1024)$$
$$\rightarrow x = 1$$

We can know that it's one bit padding, so the answer is 1.

(c)

$$2944 + x \equiv 896 (\mod 1024)$$
$$\rightarrow x = 0$$

The answer is 1024. While it is already the desired length and still requires padding.

3. State the value of the length field in SHA-512 if the length of the message is

(a) 2942 bits (5%)

(b) 2943 bits (5%)

(c) 2944 bits (5%)

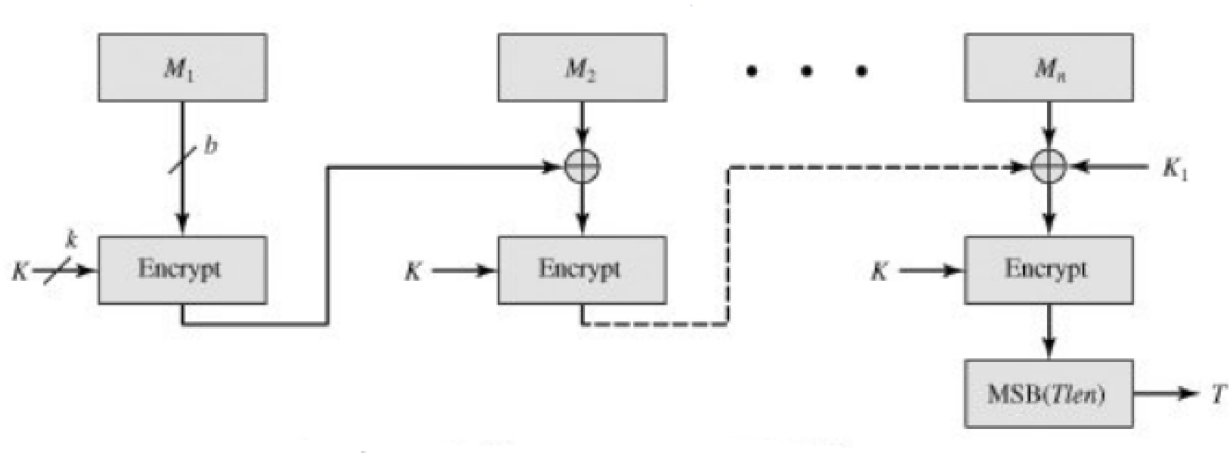
(a) 2942

(b) 2943

(c) 2944

4. In this problem, we demonstrate that for CMAC, a variant that XORs the second key after applying the final encryption doesn't work.

Let us consider this for the case of the message being an integer multiple of the block size. Then, the variant can be expressed as $VMAC(K, M) = CBC(K, M) \oplus K_1$**. Now suppose an adversary is able to ask for the MACs of three messages: the message** $0 = 0^n$**, where** n **is the cipher block size; the message** $1 = 1^n$**; and the message** $1||0$**. As a result of these three queries, the adversary gets** $T_0 = CBC(K, 0) \oplus K_1; T_1 = CBC(K, 1) \oplus K_1$ **and** $T_2 = CBC(K, [CBC(K, 1)]) \oplus K_1$**. Show that the adversary can compute the correct MAC for the (unqueried) message** $0||(T_0 \oplus T_1)$**.**



We use the above figure but put the XOR with K_1 after the final encryption. For this problem, there are two blocks to process. The output of the encryption of the first message block is $E(K, 0) = CBC(K, 0) = T_0 \oplus K_1$.This is XORed with the second message block $(T_0 \oplus T_1)$, so that the input to the second encryption is $(T_1 \oplus K_1) = CBC(K, 1) = E(K, 1)$. So the output of the second encryption is $E(K, [E(K, 1)]) = CBC(K, [CBC(K, 1)]) = T_2 \oplus K_1$. After the final XOR with K_1, we get $VMAC(K, [0||(T_0 \oplus T_1)]) = T_2$.

5. Alice want to send a single bit of information (a yes or a no) to Bob by means of a word of length 2. Alice and Bob have four possible keys available to perform message authentication. The following matrix shows the 2-bit word sent for each message under each key:

Message Key	0	1
1	00	11
2	01	10
3	10	01
4	11	00

(a) The preceding matrix is in a useful form for Alice to encrypt her message. Construct a matrix with the same information that would be more useful for Bob for decrption.

(b) What is the probability that someone else can successfully impersonate Alice?

(c) What is the probability that someone can replace an intercepted message with another message successfully?

(a)

Message Key	00	01	10	11
1	0	x	x	1
2	x	0	1	x
3	x	1	0	x
4	1	x	x	0

(b)

The attacker knows the message she wants to send, but does not know the key. Depending on the key eachmessage can have any of the 4 possible pairs of bits as a signature, with the same probability. Therefore the probability to generate the right signature is $\frac{1}{4}$.

(c)

The probability is 1. To see this it suffices to observe that if one knows the message and the signature, the key can be uniquely recovered.