Homework 4[1]

Question 1

An attacker intercepts the following ciphertext (hex encoded):

`20814804c1767293b99f1d9cab3bc3e7 ac1e37bfb15599e5f40eef805488281d`

He knows that the plaintext is the ASCII encoding of the message "Pay Bob 100$" (excluding the quotes). He also knows that the cipher used is CBC encryption with a random IV using AES as the underlying block cipher. Show that the attacker can change the ciphertext so that it will decrypt to "Pay Bob 500$". What is the resulting ciphertext (hex encoded)? This shows that CBC provides no integrity.

Question 2

Let (E,D) be an encryption system with key space K, message space $\{0,1\}^n$ and ciphertext space $\{0,1\}^s$. Suppose (E,D) provides authenticated encryption. Which of the following systems provide authenticated encryption: (as usual, we use $\|$ to denote string concatenation)

1. $E'\big((k_1,k_2),m\big) = E(k_2,\ E(k_1,m))$ and

$$D'\big((k_1,k_2),\ c\big) = \begin{cases} D(k_1,\ D(k_2,c)) & \text{if } D(k_2,c) \neq \bot \\ \bot & \text{otherwise} \end{cases}$$

2. $E'(k,m) = \big[c \leftarrow E(k,m),\ \text{output}\ \ (c,c)\,\big]$ and

$$D'(k,\ (c_1,c_2)\ ) = \begin{cases} D(k,c_1) & \text{if } c_1 = c_2 \\ \bot & \text{otherwise} \end{cases}$$

3. $E'(k,m) = \big(E(k,m),\ 0\big)$ and $D'(k,\ (c,b)\ ) = D(k,c)$

4. $E'(k,m) = \big(E(k,m),\ E(k,m)\big)$ and $D'(k,\ (c_1,c_2)\ ) = D(k,c_1)$

Question 3

If you need to build an application that needs to encrypt multiple messages using a single key, what encryption method should you use? (for now, we ignore the question of key generation and management)

1. use a standard implementation of one of the authenticated encryption modes GCM, CCM, EAX or OCB.

2. implement OCB by yourself

3. implement Encrypt-and-MAC yourself

4. use a standard implementation of randomized counter mode.

[1] `https://class.coursera.org/crypto-012/`

Question 4

Let (E,D) be a symmetric encryption system with message space M (think of M as only consisting for short messages, say 32 bytes). Define the following MAC (S,V) for messages in M:

$$S(k,m) := E(k,m) \quad ; \quad V(k,m,t) := \begin{cases} 1 & \text{if } D(k,t) = m \\ 0 & \text{otherwise} \end{cases}$$

What is the property that the encryption system (E,D) needs to satisfy for this MAC system to be secure?

1. semantic security under a chosen plaintext attack

2. authenticated encryption

3. perfect secrecy

4. semantic security

Question 5

In lecture 8.1 we discussed how to derive session keys from a shared secret. The problem is what to do when the shared secret is non-uniform. In this question we show that using a PRF with a *non-uniform* key may result in non-uniform values. This shows that session keys cannot be derived by directly using a *non-uniform* secret as a key in a PRF. Instead, one has to use a key derivation function like HKDF.

Suppose k is a *non-uniform* secret key sampled from the key space $\{0,1\}^{256}$. In particular, k is sampled uniformly from the set of all keys whose most significant 128 bits are all 0. In other words, k is chosen uniformly from a small subset of the key space. More precisely,

$$\text{for all } \ c \in \{0,1\}^{256}: \qquad \Pr[k = c] = \begin{cases} 1/2^{128} & \text{if } \mathrm{MSB}_{128}(c) = 0^{128} \\ 0 & \text{otherwise} \end{cases}$$

Let $F(k,x)$ be a secure PRF with input space $\{0,1\}^{256}$. Which of the following is a secure PRF when the key k is uniform in the key space $\{0,1\}^{256}$, but is insecure when the key is sampled from the *non-uniform* distribution described above?

1. $F'(k,x) = \begin{cases} F(k,x) & \text{if } \mathrm{MSB}_{128}(k) = 0^{128} \\ 0^{256} & \text{otherwise} \end{cases}$

2. $F'(k,x) = F(k,x)$

3. $F'(k,x) = \begin{cases} F(k,x) & \text{if } \mathrm{MSB}_{128}(k) \neq 1^{128} \\ 0^{256} & \text{otherwise} \end{cases}$

4. $F'(k,x) = \begin{cases} F(k,x) & \text{if } \mathrm{MSB}_{128}(k) \neq 0^{128} \\ 1^{256} & \text{otherwise} \end{cases}$

Question 6

In what settings is it acceptable to use *deterministic* authenticated encryption (DAE) like SIV?

1. to encrypt many records in a database with a single key when the same record may repeat multiple times.

2. when messages have sufficient structure to guarantee that all messages to be encrypted are unique.

3. when a fixed message is repeatedly encrypted using a single key.

4. to individually encrypt many packets in a voice conversation with a single key.

Question 7

Let $E(k,x)$ be a secure block cipher. Consider the following tweakable block cipher:

$$E'\big((k_1,k_2),t,x\big) = \ E(k_1,x) \bigoplus E(k_2,t).$$

Is this tweakable block cipher secure?

1. yes, it is secure assuming E is a secure block cipher.

2. no because for $t \neq t'$ we have

$$E'((k_1,k_2),t,0) \bigoplus E'((k_1,k_2),t',1) = E'((k_1,k_2),t',1) \bigoplus E'((k_1,k_2),t',0)$$

3. no because for $x \neq x'$ we have

$$E'((k_1,k_2),0,x) \bigoplus E'((k_1,k_2),0,x) = E'((k_1,k_2),0,x') \bigoplus E'((k_1,k_2),0,x')$$

4. no because for $x \neq x'$ we have

$$E'((k_1,k_2),0,x) \bigoplus E'((k_1,k_2),1,x) = E'((k_1,k_2),0,x') \bigoplus E'((k_1,k_2),1,x')$$

5. no because for $x \neq x'$ and $t \neq t'$ we have

$$E'((k_1,k_2),t,x) \bigoplus E'((k_1,k_2),t',x) = E'((k_1,k_2),t,x') \bigoplus E'((k_1,k_2),t',x)$$

Question 8

In lecture 8.5 we discussed format preserving encryption which is a PRP on a domain $\{0,\ldots,s-1\}$ for some pre-specified value of s. Recall that the construction we presented worked in two steps, where the second step worked by iterating the PRP until the output fell into the set $\{0,\ldots,s-1\}$.

Suppose we try to build a format preserving credit card encryption system from AES using **only** the second step. That is, we start with a PRP with domain $\{0,1\}^{128}$ from which we want to build a PRP with domain 10^{16}. If we only used step (2), how many iterations of AES would be needed in expectation for each evaluation of the PRP with domain 10^{16}?

1. 2^{128}

2. $10^{16}/2^{128}$

3. $2^{128}/10^{16} \approx 3.4 \times 10^{22}$

4. 4

Question 9

Let (E,D) be a secure tweakable block cipher. Define the following MAC (S,V):

$$S(k,m) := E(k,m,0) \quad ; \quad V(k,m,\text{tag}) := \begin{cases} 1 & \text{if } E(k,m,0) = \text{tag} \\ 0 & \text{otherwise} \end{cases}$$

In other words, the message m is used as the tweak and the plaintext given to E is always set to 0. Is this MAC secure?

1. yes

2. it depends on the tweakable block cipher.

3. no

Question 9

In Lecture 7.6 we discussed padding oracle attacks. These chosen-ciphertext attacks can break poor implementations of MAC-then-encrypt. Consider a system that implements MAC-then-encrypt where encryption is done using CBC with a random IV using AES as the block cipher. Suppose the system is vulnerable to a padding oracle attack. An attacker intercepts a 64-byte ciphertext c (the first 16 bytes of c are the IV and the remaining 48 bytes are the encrypted payload). How many chosen ciphertext queries would the attacker need *in the worst case* in order to decrypt the entire 48 byte payload? Recall that padding oracle attacks decrypt the payload one byte at a time.

1. 12288

2. 256

3. 12240

4. 65536