Feedback — Final Exam

Help

You submitted this exam on **Wed 14 May 2014 5:17 PM PDT**. You got a score of **13.00** out of **13.00**.

Question 1

Let (E, D) be an authenticated encryption system built by combining a CPA-secure symmetric cipher and a MAC. The system is combined with an error-correction code to correct random transmission errors. In what order should encryption and error correction be applied?

Your Answer		Score	Explanation
○ Apply the error correction code and then encrypt the result.			
○ The order does not matter -- neither one can correct errors.			
○ The order does not matter -- either one is fine.			
● Encrypt and then apply the error correction code.	✓	1.00	That is correct. The error correction code will do its best to correct random errors after which the MAC in the ciphertext will be checked to ensure no other errors remains.
Total		1.00 / 1.00	

Question 2

Let X be a uniform random variable over the set $\{0,1\}^n$. Let Y be an arbitrary random variable over the set $\{0,1\}^n$ (not necessarily uniform) that is independent of X. Define the random variable $Z = X \oplus Y$. What is the probability that Z equals 0^n?

Your Answer		Score	Explanation
○ $2/2^n$			
● $1/2^n$	✓	1.00	The probability is $1/2^n$. To see why, observe that whatever Y is, the probability that $Z = X \oplus Y = 0^n$is the same as the probability that $X = Y$ which is exactly $1/2^n$ because X is uniform.
○ $1/n^2$			
○ $1-(1/2^n)$			
Total		1.00 / 1.00	

Question 3

Suppose (E_1, D_1) is a symmetric cipher that uses 128 bit keys to encrypt 1024 bit messages. Suppose (E_2, D_2) is a symmetric cipher that uses 128 bit keys to encrypt 128 bit messages. The encryption algorithms E_1 and E_2 are deterministic and do not use nonces. Which of the following statements is true?

Your Answer		Score	Explanation
☑ (E_1, D_1) can be one-time semantically secure.	✓	0.25	Yes, for example (E_1, D_1) can be a secure stream cipher.
☑ (E_2, D_2) can be one-time semantically secure and perfectly secure.	✓	0.25	Yes, for example (E_2, D_2) can be the one time pad.
□ (E_1, D_1) can be perfectly secure.	✓	0.25	The statement is incorrect: for (E_1, D_1) the keys are too short to provide perfect

			secrecy.
□ (E_1, D_1) can be semantically secure under a chosen plaintext attack.	✓	0.25	The statement is incorrect: (E_1, D_1) is deterministic and uses no nonces
Total		1.00 / 1.00	

Question 4

Which of the following statements regarding CBC and counter mode is correct?

Your Answer		Score	Explanation
● CBC mode encryption requires a block cipher (PRP), but counter mode encryption only needs a PRF.	✓	1.00	Yes, CBC needs to invert the PRP for decryption, while counter mode only needs to evaluate the PRF in the forward direction for both encryption and decryption. Therefore, a PRF is sufficient for counter mode.
○ Both counter mode and CBC mode can operate just using a PRF.			
○ counter mode encryption requires a block cipher (PRP), but CBC mode encryption only needs a PRF.			
○ Both counter mode and CBC mode require a block cipher (PRP).			
Total		1.00 / 1.00	

Question 5

Let $G : X \to X^2$ be a secure PRG where $X = \{0,1\}^{256}$. We let $G(k)[0]$ denote the left half of the output and $G(k)[1]$ denote the right half. Which of the following statements is true?

Your Answer		Score	Explanation
○ $F(k,m) = m \oplus k$ is a secure PRF with key space and message space X.			
○ $F(k,m) = G(m)[0] \oplus k$ is a secure PRF with key space and message space X.			
○ $F(k,m) = G(k)[0] \oplus m$ is a secure PRF with key space and message space X.			
● $F(k,m) = G(k)[m]$ is a secure PRF with key space X and message space $m \in \{0,1\}$.	✓	1.00	Yes, since the output of $G(k)$ is indistinguishable from random, the left and right halves are indistinguishable from random independent values.
Total		1.00 / 1.00	

Question 6

Let (E, D) be a nonce-based symmetric encryption system (i.e. algorithm E takes as input a key, a message, and a nonce, and similarly the decryption algorithm takes a nonce as one of its inputs). The system provides chosen plaintext security (CPA-security) as long as the nonce never repeats. Suppose a single encryption key is used to encrypt 2^{32} messages and the nonces are generated independently at random for each encryption, how long should the nonce be to ensure that it never repeats with high probability?

Your Answer		Score	Explanation
○16 bits			
●128 bits	✓	1.00	Yes, the probability of repetition after 2^{32} samples is negligible.
○32 bits			
○48 bits			
Total		1.00 / 1.00	

Question 7

Same as question 6 except that now the nonce is generated using a counter. The counter resets to 0 when a new key is chosen and is incremented by 1 after every encryption. What is the shortest nonce possible to ensure that the nonce does not repeat when encrypting 2^{32} messages using a single key?

Your Answer		Score	Explanation
○128 bits			
● 32 bits	✓	1.00	Yes, with 32 bits there are 2^{32} nonces and each message will use a different nonce.
○ 16 bits			
○the nonce must be chosen at random, otherwise the system cannot be CPA secure.			
Total		1.00 / 1.00	

Question 8

Let (S, V) be a deterministic MAC system with message space M and key space K. Which of the following properties is implied by the standard MAC security definition?

Your Answer	Score	Explanation
○ The function $S(k, m)$ is a secure PRF.		
○Given a key k in K it is difficult to find distinct messages m_0 and m_1 such that $S(k, m_0) = S(k, m_1)$		
●Given m and $S(k, m)$ it is difficult to compute k.	✓ 1.00	yes, otherwise the attacker can easily mount an existential forgery.
○$S(k, m)$ preserves semantic security of m. That is, the adversary learns nothing about m given $S(k, m)$.		
Total	1.00 / 1.00	

Question 9

Let $H : M \to T$ be a collision resistant hash function where $|T|$ is smaller than $|M|$. Which of the following properties is implied by collision resistance?

Your Answer	Score	Explanation
○For all m in M, $H(m)$ must be shorter than m.		
○ it is difficult to find m_0 and m_1 such that $H(m_0) = H(m_1) + 1$ (here we treat the outputs of H as integers)		
●Given a tag $t \in T$ it is difficult to construct $m \in M$ such that $H(m) = t$	✓ 1.00	yes, if these were easy then the attacker could easily find collisions.
○ $H(m)$ preserves semantic security of		

m (that is, given $H(m)$ the attacker learns nothing about m).		
Total		1.00 / 1.00

Question 10

Recall that when encrypting data you should typically use a symmetric encryption system that provides authenticated encryption. Let (E, D) be a symmetric encryption system providing authenticated encryption. Which of the following statements is implied by authenticated encryption?

Your Answer		Score	Explanation
☑ (E, D) provides chosen-ciphertext security.	✓	0.25	yes, we showed this in class.
☑Given m and $E(k, m)$ the attacker cannot create a valid encryption of $m + 1$ (here we treat plaintexts as integers)	✓	0.25	yes, otherwise the system would not have ciphertext integrity.
□ Given $c = E(k, m)$for some secret k, m, the attacker cannot find k', m' such that $c = E(k', m')$.	✓	0.25	The statement is incorrect: there are no guarantees about the hardness of finding keys k' with special properties. For example, it is possible to build a GCM-like system where finding k' and m' is easy, despite the system providing authenticated encryption.
□Given k, m and $E(k, m)$ the attacker cannot create a valid encryption of	✓	0.25	The statement is incorrect: once the attacker is given k the system has no security.

$m+1$under key k. (here we treat plaintexts as integers)			
Total		1.00 / 1.00	

Question 11

Which of the following statements is true about the basic Diffie-Hellman key-exchange protocol.

Your Answer		Score	Explanation
□The protocol is based on the concept of a trapdoor function.	✓	0.25	The statement is incorrect: Diffie-Hellman does not use trapdoor functions. It is based on the exponentiation function $f(x) = g^x$ and the fact that $(g^a)^b = (g^b)^a$. The exponentiation function in $\mathbb{Z}_p^*$ does not have a trapdoor (as far as we know).
□ As with RSA, the protocol only provides eavesdropping security in the group $\mathbb{Z}_N^*$ where N is an RSA modulus.	✓	0.25	The statement is incorrect: Diffie-Hellman works in any group where the Hash Diffie-Hellman problem holds.
☑The protocol can be converted to a public-key encryption system called the ElGamal public-key system.	✓	0.25	yes, that is correct.
☑The protocol provides security against eavesdropping in any finite group in which the Hash	✓	0.25	yes, in any such group the hash of the Diffie-Hellman secret g^{ab} can be used as a shared secret.

Diffie-Hellman (HDH) assumption holds.			
Total		1.00 / 1.00	

Question 12

Suppose $n+1$ parties, call them $B, A_1, \ldots, A_n$ wish to setup a shared group key. They want a protocol so that at the end of the protocol they all have a common secret key k, but an eavesdropper who sees the entire conversation cannot determine k. The parties agree on the following protocol that runs in a group G of prime order q with generator g:

- for $i = 1, \ldots, n$party A_i chooses a random a_i in $\{1, \ldots, q\}$and sends to Party B the quantity $X_i \leftarrow g^{a_i}$.
- Party B generates a random b in $\{1, \ldots, q\}$and for $i = 1, \ldots, n$responds to Party A_i with the messages $Y_i \leftarrow X_i^b$.

The final group key should be g^b. Clearly Party B can compute this group key. How would each Party A_i compute this group key?

Your Answer		Score	Explanation
○Party A_i computes g^b as $Y_i^{a_i}$			
●Party A_i computes g^b as Y_i^{1/a_i}	✓	1.00	Yes, $Y_i^{1/a_i} = g^{(ba_i)/a_i} = g^b$.
○ Party A_i computes g^b as Y_i^{-1/a_i}			
○ Party A_i computes g^b as $Y_i^{-a_i}$			
Total		1.00 / 1.00	

Question 13

Recall that the RSA trapdoor permutation is defined in the group $\mathbb{Z}_N^*$ where N is a product of two large primes. The public key is (N, e) and the private key is (N, d) where d is the inverse of

e in $\mathbb{Z}^*_{\varphi(N)}$.

Suppose RSA was defined modulo a prime p instead of an RSA composite N. Show that in that case anyone can compute the private key (N,d) from the public key (N,e) by computing:

Your Answer		Score	Explanation
● $d \leftarrow e^{-1} \pmod{p-1}$	✓	1.00	yes, that is correct.
○ $d \leftarrow e^{-1} \pmod{p}$.			
○ $d \leftarrow e^{2} \pmod{p}$.			
○ $d \leftarrow e^{-1} \pmod{p^2}$.			
Total		1.00 / 1.00	