Final

May 2, 2016, 2:00–4:30 PM

There are seven problems each worth five points for a total of 35 points. Show all your work, partial credit will be awarded. Space is provided on the test for your work; if you use a blue book for additional workspace, sign it and return it with the test.

No notes, no collaboration. Please do all computations by hand, no calculators, cell phones, or any other device or method that permits communication or calculation.

Name: _____

Problem	Credit
1	
2	
3	
4	
5	
6	
7	
Total	

1. *Eavesdropping security*

   Consider the substitution cipher. Let π be a secretly chosen permutation of letters in an alphabet. The encryption of a word m written as a sequence of letters $m = w_1 w_2 \dots w_l$, is the ciphertext $c = \pi(w_1)\pi(w_2)\dots\pi(w_k)$.

   Show that a substitution cipher is not secure under adversarial indistinguishability (i.e. eavesdropping security).

   The definition of *adversarial indistinguishability* is recalled on page 10 of test.

   Hint: A reduction is not needed.

2. *CPA security*

   The Enigma cipher was *involutory*, meaning twice encryption is the identity, $E(E(x)) = x$. This was done to simplify the machinery — encryption and decryption are the same function.

   Show that no involutory cipher is secure under CPA indistinguishability.

   The definition of *CPA indistinguishability* is recalled on page 10 of test.

   Hint: A reduction is not needed.

   Hint: Because no deterministic cipher is secure under CPA indistinguishability, you must suppose that E is not deterministic. That is, $E(x)$ can be one of a large set of values, and on each invocation of E one value chosen at random.

3. *CCA security*

   Counter Mode encryption uses a pseudorandom function F_k, where k is the secret key, and encrypts the message $m_1, m_2, \ldots$ as,

   $$r, m_1 \oplus F_k(r+1), m_2 \oplus F_k(r+2), \ldots$$

   where r is a random number chosen independently for each encryption.

   It is known that Counter Mode is secure under CPA indistinguishability. Show that it is <u>not</u> secure under CCA indistinguishability.

   The definition of *CCA indistinguishability* is recalled page 11 of test.

   Hint: A reduction is not needed.

4. *MAC security*

   Given a pseudorandom function F_k, the MAC on message m is $F_k(m)$.

   This MAC is unforgeable in the Random Oracle Model. In this model tags are assigned to messages by the oracle independently at random, and the two key holders agree on the tags by reference to the common oracle.

   Note that the size of the message m must be equal to the block length of F_k. Consider an extension of the construction.

   Assume the length of m be a multiple of the block length of F_k. Write m as:

   $$m = m_1|m_2|\ldots|m_k$$

   where each m_i is of the block length of F. Calculate the MAC by:

   $$F_k(\oplus_{i=1,\ldots,k} m_i)$$

   Show that this construction is <u>not</u> secure against message authentication forgery.

   The definition of *message authentication forgery* is recalled page 11 of test.

   Hint: A reduction is not needed.

5. *Pubilc Key RSA*

   Let the two distinct primes for an RSA cryptosystem be 7 and 11. Let the public exponent be 17.

   (a) State the public key, i.e. the information made public.

   (b) State the private key, i.e. the information kept private.

   (c) Give the encryption of the number 2.

   (d) Show decryption of 2.

   Show your work. Parts (a), (b) and (c) should be easy to hand-calculate. Part (d) might not be that easy to hand-calculate (save for if you have time).

6. *Diffie-Hellman on Elliptic Curves*

   Alice and Bob want to share a point on the elliptic curve,

   $$y^2 = x^3 + 2x + 2 \bmod 17$$

   The group of points on this curve are generated by the point $P = (5, 1)$

   Alice and Bob can communicate only over a public channel and do not want any eavesdropper to know the shared point. They agree to use Diffie-Hellman, using the public parameters the curve above and generator P.

   Alice says $(13, 7)$ and Bob says $(9, 1)$. What is the shared point?

   Note: The elliptic curve cheat sheet on page 12 of the test gives helpful computations for this curve.

7. *ECDSA signatures*

The Elliptic Curve Digital Signature Algorithm is a standard for digital signatures that follows the structure of a Fiat-Shamir signature. In this problem,

The public parameters:

(a) The elliptic curve is $y^2 = x^3 + 2x + 2 \pmod{17}$.

(b) The point $P = (5, 1)$ is the selected generator the group of points on the curve.

(c) The number of points on the curve and generate by P is $q = 19$.

(d) We suppose a cryptographically strong hash function $H : \{0,1\}^* \to \mathbf{Z_{19}}$ from messages to numbers.

(e) We use the function F from points to numbers, which simply extracts the first coordinate $F\big((x, y)\big) = x$.

The private parameter:

(f) The signer chooses and keeps secret a random $\sigma \in \mathbf{Z_{19}}$ and publishes the point $Q = \sigma P$.

Sign/Verify:

(g) On message m, signer selects a random $k \in \mathbf{Z_{19}^*}$ and output the signature:

$$(r, s) = \big(\, r, k^{-1}(H(m) + \sigma r)\,\big) \pmod{19}$$

where $r = F(kP)$.

(h) On message m and signature (r, s) the verifier checks for equality:

$$r \stackrel{?}{=} F\big(\; H(m)s^{-1}P + rs^{-1}Q \;\big)$$

where the coefficients (e.g. s^{-1}) are computed in $\mathbf{Z_{19}}$.

Please answer,

(a) Show that any properly signed message will verify.

(b) Show that $(7, 8)$ is the correct signature on message $H(m) = 7$ when $Q = (9, 16)$. (Show all relevant steps.)

Note: The elliptic curve cheat sheet on page 12 of the test gives helpful computations for this curve.

Workspace for problem 7

Security Definitions

Definition 0.1 (Adversarial indistinguishability experiment)

(a) The adversary A outputs a pair of messages m_0, m_1.

(b) A key k is generated by running $GEN(1^n)$. A uniform bit $b \in \{0,1\}$ is chosen, and then a ciphertext $c = ENC_k(m_b)$ is computed and given to A.

(c) The adversary A outputs a bit b'.

(d) If $b = b'$ then the adversary A succeeds. Otherwise, it fails.

Definition 0.2 (CPA indistinguishability experiment)

(a) A key k is generated by running $GEN(1^n)$.

(b) The adversary A is given input 1^n and oracle access to $ENC_k()$, and outputs a pair of messages m_0, m_1 of the same length.

(c) A uniform bit $b \in \{0,1\}$ is chosen, and then a ciphertext $c = ENC_k(m_b)$ is computed and given to A.

(d) The adversary A continues to have oracle access to $ENC_k()$, and outputs a bit b'.

(e) If $b = b'$ then the adversary A succeeds. Otherwise, it fails.

Security Definitions (continued)

Definition 0.3 (CCA indistinguishability experiment)

(a) A key k is generated by running $GEN(1^n)$.

(b) The adversary A is given input 1^n and oracle access to $ENC_k()$ and $DEC_k()$, and outputs a pair of messages m_0, m_1 of the same length.

(c) A uniform bit $b \in \{0,1\}$ is chosen, and then the challenge ciphertext $c = ENC_k(m_b)$ is computed and given to A.

(d) The adversary A continues to have oracle access to $ENC_k()$ and $DEC_k()$, but is not allowed to query DEC_k on the challenge ciphertext c, and outputs a bit b'.

(e) If $b = b'$ then the adversary A succeeds. Otherwise, it fails.

Definition 0.4 (Message authentication forgery experiment)

(a) A key k is generated by running $GEN(1^n)$.

(b) The adversary A is given input 1^n and oracle access to $MAC_k()$ and outputs (m, t). Let Q denote the set of all queries that A has asked of its oracle.

(c) Adversary A succeeds if and only if:

i. $VRFY(m, t) = 1$, and

ii. $m \notin Q$.

Elliptic curve cheat sheet

Group law for the elliptic curve

$$\begin{aligned} y^2 &= x^3 + ax + b \pmod p \\ (x_3, y_3) &= (x_1, y_1) + (x_2, y_2) \\ s &= \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} \pmod p, P \neq Q \text{ and } x_2 \neq x_1 \\ \frac{3x_1^2 + a}{2y_1} \pmod p, P = Q \text{ and } y_1 \neq 0 \end{cases} \\ x_3 &= s^2 - x_1 - x_2 \pmod p \\ y_3 &= s(x_1 - x_3) - y_1 \pmod p \end{aligned}$$

In the excluded cases, the sum is the point at infinity. Note the curve must be non-singular: $4a^3 - 27b^2 \neq 0 \pmod p$.

Curve used in problems

For the curve $y^2 = x^3 + 2x + 2 \pmod{17}$, the orbit of $(5, 1)$ is as follows:

index	*point*
1	(5,1)
2	(6,3)
3	(10,6)
4	(3,1)
5	(9,16)
6	(16,13)
7	(0,6)
8	(13,7)
9	(7,6)
10	(7,11)
11	(13,10)
12	(0,11)
13	(16,4)
14	(9,1)
15	(3,16)
16	(10,11)
17	(6,14)
18	(5,16)
19	O