Name (First, Last):
UCI ID Number:

• Please write (clearly) your name and student ID on the top of each page.
• Make sure you have 12 pages with 5 sections of questions.
• Only pens, pencils and erasers are allowed. No other items can be present (e.g., notes, books, smartphones, tablets, laptops ...etc.).
• No communication or interaction with other students is allowed.
• Raise your hand if you have a question.

<table>
<thead>
<tr>
<th>Question</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Points</td>
<td>15</td>
<td>10</td>
<td>9</td>
<td>9</td>
<td>9</td>
<td>52</td>
</tr>
<tr>
<td>Score:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
1 (1.5pt each) Multiple Choice Questions - mark a single answer

1. Which of the following is an advantage of public-key cryptography over symmetric-key cryptography?
   A. Public-key cryptography provides more security services
   B. Public-key cryptography does not rely on conjectured hardness of certain computational problems
   C. Public-key cryptography has higher throughput
   D. Public-key cryptography has shorter key size
   E. All of the above

2. Suppose you receive a ciphertext in Polish consisting of 5 unique letters and know that this ciphertext is produced by a Substitution Cipher. How many possible plaintexts are there that could have produced this ciphertext? Assume that there are 32 letters in the Polish alphabet.
   A. $32 \cdot 31 \cdot 30 \cdot 29 \cdot 28$
   B. $32^5$
   C. $5^{32}$
   D. $32!$
   E. None of the above

3. Which of the following cryptographic algorithms should be used for ensuring integrity and authenticity of a message?
   A. SHA1
   B. SHA1-based HMAC
   C. RSA encryption
   D. AES-based ECB mode
   E. None of the above

4. Based on current knowledge, which of the following problems is NOT “difficult” to solve? A problem is considered to be difficult to solve when there is no known efficient algorithm that solves it.
   A. Given a large prime $p$ and an integer $a$, finding an integer $x$ such that $a \cdot x = 1 \mod p$
   B. Given a large composite $n$, finding all prime factors of $n$
   C. Given an integer $a$ and a large composite $n$, finding an integer $x$ such that $x^2 = a \mod n$
   D. Given integers $a$ and $b$ and a large prime $p$, finding an integer $x$ such that $a^x = b \mod p$
   E. None of the above

5. Denote $l$ as the effective key length for a block cipher $E()$. What is the effective key length of 4-E: $C = E(K_1, E(K_2, E(K_3, E(K_4, P))))$? Assume $K_i$’s are keys, $P$ is a plaintext and $C$ is a ciphertext. (Hint: do not forget about Meet-in-the-Middle attack)
   A. $l$
   B. $2 \cdot l$
   C. $3 \cdot l$
   D. $4 \cdot l$
   E. None of the above
6. Using the birthday paradox, on average, how many trials does it take (approximately) to find a collision on an n-bit hash with \( \geq 0.5 \) probability?
   A. \( \sqrt{\log(n)} \)
   B. \( \sqrt{n} \)
   C. \( \sqrt{2^n} \)
   D. \( 2^n/2 \)
   E. None of the above

7. Consider the following system of two equations (congruences):
   \[
   x = 12 \mod 29
   \]
   \[
   x = 7 \mod 15
   \]
   According to Chinese Remainder Theorem (CRT), which of the following is true about \( x \)?
   A. \( x \) has no solution in \((\mod 29 \cdot 15)\)
   B. \( x \) has exactly one solution in \((\mod 29 \cdot 15)\)
   C. \( x \) has more than one solution in \((\mod 29 \cdot 15)\)
   D. \( x \) has four solutions in \((\mod 29 \cdot 15)\) because there are two equations
   E. None of the above

8. Suppose Alice and Bob want to establish a shared secret key by executing the Diffie-Hellman key exchange protocol (consider the textbook version discussed in class). First, they agree to use a modulus \( p = 13 \) and a generator \( g = 7 \). Alice then chooses \( a \) as her secret integer and sends Bob \( A = g^a \mod p = 8 \). Suppose Bob chooses 3 as his secret integer and sends Alice \( B = g^3 = 5 \mod p \). What is a shared secret between Alice and Bob?
   A. 1
   B. 5
   C. 6
   D. 12
   E. None of the above

9. What is an RSA signature for a message \( m = 4 \)? Assume the following RSA parameters: a private exponent \( d = 17 \) and a composite \( n = 21 \). (Hint: Lagrange’s Theorem implies that \( a^{\phi(n)} = 1 \mod n \) when \( \gcd(a, n) = 1 \).)
   A. 1
   B. 4
   C. 16
   D. 20
   E. None of the above

10. Suppose a prime \( p = 3 \mod 4 \) and \( a \in \mathbb{Z}_p \). Which of the following is equivalent to a square root of \( a \mod p \)?
    A. \( a^{p-1} \mod p \)
    B. \( a^{(p+1)/4} \mod p \)
    C. \( a^{(p+1)/2} \mod p \)
    D. \( a^{(p-1)/2} \mod p \)
    E. All of the above
2 (2pts each) Fill in the Blanks

1. Using the Cipher Feedback (CFB) mode, a Message Authentication Code (MAC) of a message $m$ can be created by

   encrypting $m$ using CFB mode and using the last block as MAC.

2. The AES cipher in Electronic Code Book (ECB) mode should not be used to encrypt bulk data (i.e., multiple blocks) because

   it exposes duplicate plaintext blocks.

3. $\Phi(237) = 2 \times 78 = 156$ (Hint: 237 is a product of two primes, one of which is very small).

4. There are 6, which is $\{1, 2, 4, 5, 7, 8\}$ elements in $\mathbb{Z}_9^*$ (Hint, $\mathbb{Z}_n^*$ is a set of positive integers (mod $n$) relatively prime to $n$).

5. Using ElGamal Public Key Cryptosystem, a ciphertext of a message $m$ is: $[k, c] = [b^k \mod p, m \cdot y^r \mod p]$.

   The formula for decrypting $[k, c]$ is $(k^x)^{-1} \cdot c \mod p$.

   Recall that the parameters of ElGamal Public Key Cryptosystem are: $p$ is a large prime, $b$ is a generator in $\mathbb{Z}_p$, $x$ is a private exponent and $y = b^x \mod p$ is the public key.
3 Block Cipher

Consider the “Plaintext Feedback” (PFB) mode where the encryption formula for ciphertext block $C_i$ is:

$$C_i = E_K(P_i) \oplus C_{i-1}, \quad C_0 = IV$$

and $E()$ can be any strong block cipher, e.g., AES.

Answer the following questions.

(a) (3 pts) What is the formula for decrypting ciphertext block $C_i$?

(b) (3 pts) Explain the precise consequence of the loss of ciphertext block $C_i$. Assume a decryptor is aware of that loss (i.e., knows the index, $i$, of the lost block).

(c) (3 pts) Are there any security problems in PFB mode? If so, identify one problem and briefly justify your answer. If not, explain why there are no problems.

Solution:

(a) $P_i = D_K(C_i \oplus C_{i-1})$

(b) $P_i$ and $P_{i+1}$ are lost.

(c) It exposes IV and duplicate plaintext blocks, e.g., $P$ consists of three plaintext blocks and all of them are the same. $P = P_1 \parallel P_2 \parallel P_3 = P_1 \parallel P_1 \parallel P_1$, then $E_K(P) = C_1 \parallel IV \parallel C_1$, where $C_1 = E_K(P_1) \oplus IV$. 
Name (First, Last):
UCI ID Number:

Solution:
4 ElGamal Signature Scheme

(a) (3 pts) Explain how an adversary can recover the secret key (i.e., $x$) when the signer reuses the same random number $r$ for two different messages. State your assumptions.

(b) (3 pts) Consider a variant of ElGamal signature scheme where $m$ and $r$ are swapped in the signing algorithm, i.e., a digital signature of message $m$ is: $[k, c] = [b^r \mod p, (r - x \cdot k) \cdot m^{-1} \mod p - 1]$. What is the formula for verifying the signature $[k, c]$ in this variant?

(c) (3 pts) Are there any security problems in the variant, described in (b)? If so, identify one and briefly justify it. If not, explain why not. (Note that in this question, you cannot assume that the signer will reuse the same random number $r$.)

(Hint: This is a digital signature scheme, so a message needs to be sent along with its signature. Or simply put, in this scheme, a message is always visible to public and thus also to the adversary.)
Solution:

(a) Consider two signatures \([k, c_1]\) and \([k, c_2]\) for messages \(m_1\) and \(m_2\) respectively.

\[
c_1 - c_2 = (m_1 - x \cdot k - m_2 + x \cdot k) \cdot r^{-1} \mod p - 1
\]

\[
(c_1 - c_2) \cdot r = (m_1 - m_2) \mod p - 1
\]

Assume \((c_1 - c_2)\) has an inverse in \(\mod p - 1\). \(r = (c_1 - c_2)^{-1} \cdot (m_1 - m_2) \mod p - 1\)

Once you learn \(r\), it is easy to find \(x\):

\[
x = (m_1 - c_1 \cdot r) \cdot k^{-1} \mod p - 1.
\]

(b) \(k = b^{mc} \cdot y^k \mod n\). This is because \(b^{mc} \cdot y^k = b^{r-xk} \cdot y^k = b^r \cdot b^{-xk} \cdot b^{xk} = b^r = k \mod n\).

(c) An adversary can forge a signature of any message if he knows one legitimate signature of one message. A signature of any message \(m'\), given \(m\) and \([k, c]\) is \([k, c \cdot m' \cdot m'^{-1}] = [k, (r - x \cdot k) \cdot m'^{-1}].\)
5 Zero Knowledge with RSA

Consider the following identification scheme (known as Guillou-Quisquater scheme) which is also another example of a zero-knowledge proof. For simplicity, assume there is only one honest prover and one honest verifier in this scheme.

The scheme starts by having a trusted third party (TTP) generate a large composite number $n$, which is a product of two primes $p$ and $q$. In addition, TTP generates a public RSA exponent $e$ and a private RSA exponent $d$. TTP publishes $n$ and $e$ but keeps $p$, $q$, and $d$ secret. Suppose a prover’s public identity (e.g., name or phone number) is $I$. TTP then gives the prover the value $B = I^{-d} \mod n$, which is served as his/her secret.

The identification protocol then consists of 4 steps and can be described as follows:

1. The prover (PRV) chooses a random number $r \in \mathbb{Z}_n^*$ and computes $T = r^e \mod n$. PRV then sends $T$ to the verifier (VRF) and keeps $r$ secret.
2. VRF chooses a random number $c \in \{0, 1, ..., e - 1\}$ and sends $c$ to PRV.
3. PRV computes $t = r \cdot B^c \mod n$ and sends $t$ to VRF.
4. VRF accepts the identification if and only if $T = I^c \cdot t^e \mod n$.

Question:

(a) (3 pts) Mathematically show that $T = I^c \cdot t^e \mod n$.

(b) (3 pts) Suppose VRF knows a factor modulus ($p$ and $q$). Explain how VRF can learn PRV’s secret (i.e., $B$) from this protocol. (Hint: $e$ is a public RSA exponent and $I$ is PRV’s public identity)

(c) (3 pts) Suppose a malicious prover (PRV$_m$) knows $c$ ahead of time (i.e., before the start of the protocol). Explain how PRV$_m$ can impersonate PRV without needing to know $B$, $d$, $p$ or $q$. 


Solution:

(a) \( T = r^e = (t \cdot B^{-c})^e = t^e \cdot B^{-ec} = t^e \cdot I^{edc} = t^e \cdot I^e \mod n \) since \( e \cdot d = 1 \mod (p - 1)(q - 1) \).

(b) Since \( e \) is public, learning \( p \) and \( q \) will allow you to find \( e^{-1} \) or \( d \) via EEA. Once you find \( d \), you can compute \( q = I^d \mod n \) and thus \( B = q^{-1} = (I^d)^{-1} = I^{-d} \mod n \) since \( I \) is also public.

(c) If PRV \(_m\) knows \( c \) in advance, he will then send \( T = I^c \mod n \) and \( t = 1 \) to VRF in step 1 and 3 respectively. VRF accepts the identification because \( t^e \cdot I^c = I^c = T \mod n \).
Name (First, Last):
UCI ID Number:

Solution: