CS548 Advanced Information Security Final Exam

Type of exam: Take home exam
Deadline: May 20th 16:00
Submission: TA (junhyunv@kaist.ac.kr) by e-mail.

(Note)
* Your program source and execution result (e.g. screen shot) of problems 3, 4 and 7 must be attached.

1. Consider the following linear recurrence over \( \mathbb{Z}_2 \) of degree four:
   \[
   z_{i+4} = (z_i + z_{i+1} + z_{i+2} + z_{i+3}) \mod 2,
   \]
   \( i \geq 0 \). For each of the 16 possible initialization vectors \( \langle z_i, z_{i+1}, z_{i+2}, z_{i+3} \rangle \in (\mathbb{Z}_2)^4 \), determine the period of the resulting keystream. (1.18, p.40)

2. Suppose we are told that the plaintext 
   \textbf{breathtaking}
   yields the ciphertext
   \textbf{RUPOTENTOIFV}
   where the Hill Cipher is used (but \( m \) is not specified). Determine the encryption matrix. (1.23, p.42)

3. Suppose that we have the following 128-bit AES key, given in hexadecimal notation:
   \textbf{2B7E151628AED2A6ABF7158809CF4F3C}
   Construct the complete key schedule arising from this key. (3.5, p.114)

4. Compute the encryption of the following plaintext (given in hexadecimal notation) using the 10-round AES:
   \textbf{3243F6A8885A308D313198A2E0370734}
   Use the 128-bit key from the previous exercise. (3.6, p.115)

5. Prove that the RSA Cryptosystem is insecure against a chosen ciphertext attack. In particular, given a ciphertext \( y \), describe how to choose a ciphertext \( \hat{y} \neq y \), such that knowledge of the of the plaintext \( \hat{x} = d_K(\hat{y}) \), allows \( x = d_K(y) \), to be computed. (5.14, p.228)
6. This exercise illustrates another example of a protocol failure (due to Simmons) involving the RSA Cryptosystem; it is called the “common modulus protocol failure.” Suppose Bob has an RSA Cryptosystem with modulus $n$ and encryption exponent $b_1$, and Charlie has an RSA Cryptosystem with (the same) modulus $n$ and encryption exponent $b_2$. Suppose also that $gcd(b_1, b_2) = 1$. Now, consider the situation that arises if Alice encrypts the same plaintext $x$ to send to both Bob and Charlie. Thus, she computes $y_1 = x^{b_1} \mod n$ and $y_2 = x^{b_2} \mod n$, and then she sends $y_1$ to Bob and $y_2$ to Charlie. Suppose Oscar intercepts $y_1$ and $y_2$, and performs the computations indicated in Algorithm 5.16. (5.16, p.229)

**Algorithm 5.16**: RSA COMMON MODULUS DECRYPTION($n, b_1, b_2, y_1, y_2$)

1. $c_1 \leftarrow b_1^{-1} \mod b_2$
2. $c_2 \leftarrow (c_1 b_1 - 1) / b_2$
3. $x_1 \leftarrow y_1^{c_1} (y_2^{c_2})^{-1} \mod n$

return $(x_1)$

(a) Prove that the value $x_1$ computed in Algorithm 5.16 is in fact Alice’s plaintext $x$. Thus Oscar can decrypt the message Alice sent, even though the cryptosystem may be “secure.

(b) Illustrate the attack by computing $x$ by this method if $n = 18721$, $b_1 = 43$, $b_2 = 7717$, $y_1 = 12677$, and $y_2 = 14702$.

7. Implement SHANKS’ ALGORITHM for finding discrete logarithms in $\mathbb{Z}_p^*$, where $p$ is prime and $\alpha$ is primitive element modulo $p$. Use your program to find $log_{106} 12375$ in $\mathbb{Z}_{24691}^*$ and $log_{26} 24388$ in $\mathbb{Z}_{458009}^*$. (6.1, p.275)

8. The field $\mathbb{F}_{2^5}$ can be constructed as $\mathbb{Z}_2[x]/(x^5 + x^2 + 1)$. Perform the following computations in this field. (6.11, p.277)

(a) Compute $(x^4 + x^2) \times (x^3 + x + 1)$.
(b) Using the extended Euclidean algorithm, compute $(x^3 + x^2)^{-1}$.
(c) Using the square-and-multiply algorithm, compute $x^{25}$.

9. Suppose Alice is using the ElGamal Signature Scheme with $p = 31847, \alpha = 5, \beta = 25703$. Compute the values of $k$ and $\alpha$ (without solving an instance of the Discrete Logarithm problem), given the signature $(23972, 31396)$ for the message $x = 8990$ and the signature $(23972, 20481)$ for the message $x = 31415$. (7.1, p.318)
10. Suppose Alice is using the Schnorr Identification Scheme where \( q = 1201, \ p = 122503, \ t = 10 \) and \( \alpha = 11538 \). (9.8, p.390)

(a) Verify that \( \alpha \) has order \( q \) in \( \mathbb{Z}_p^\times \).

(b) Suppose that Alice’s secret exponent is \( a = 357 \). Compute \( v \).

(c) Suppose that \( k = 868 \). Compute \( y \).

(d) Suppose that Bob issues the challenge \( r = 501 \). Compute Alice’s response \( y \).

(e) Perform Bob’s calculations to verify \( y \).