Homework 02 Solutions

ECE 443/518, Fall 2025

1. *(1 point)* Solve Problem 12.3 (p329 in Understanding Cryptography).

   Answer:

   1) Assume the stream cipher works by xoring the key stream with the plaintext. If the attacker knows x and thus $h(x)$, then the plaintext is known. Now the key stream can be recovered by xoring the plaintext and the ciphertext. With the key stream, the attacker can encrypt any other plaintext having the same length.
   2) If the hash function is replaced with a MAC function then the above attack doesn't apply since with the knowledge of the MAC key k_2, the attacker cannot generate correct MAC for any other message x'.

2. *(1 point)* Alice chooses $p = 11$ and $q = 19$ to setup her RSA keys.

   A. Show that $e = 5$ is NOT a valid choice.

   B. Show that $e = 7$ is a valid choice. What is the public key and what is the corresponding private key?

   C. Suppose Bob want to send the message $x = 10$ to Alice using the keys generated in the question B. Show how Bob computes the ciphertext y and how Alice decrypts y.

   Answer:

   A) $gcd(5, (p-1)(q-1)) = gcd(5, 10*18) = 5 \neq 1$. So $e = 5$ is not a good choice.

   B) $gcd(5, (p-1)(q-1)) = gcd(5, 10*18) = 1$. So $e = 7$ is a good choice. The public key is $(n, e) = (209, 7)$.

   To obtain private key we need to solve $7d \equiv 1 \pmod{180}$. Apply the EEA algorithm we have $d = 103$ so the private key is $(p, q, d) = (11, 19, 103)$.

   C) For Bob, $y \equiv x^e \equiv 10^7 \equiv 186 \pmod{209}$.

   For Alice, $x \equiv y^d \equiv 186^{103} \equiv 186^3 * (186^4)^{25} \equiv 164 * 199^{25} \equiv 32 * 177^6 \equiv 32 * 45^2 \equiv 10 \pmod{209}$.

   (Hint: your 10-digit calculator should be able to compute numbers like 10^7 and 186^4 accurately.)

3. *(1 point)* Bob setups his RSA key using $p = 13$, $q = 17$, and $e = 5$.

   A. What is the public key and what is the corresponding private key?

   B. For the question 3.C, if Bob want to sign his message $x = 10$, show how Bob computes the signature and how Alice verifies it.

   Answer:

   A) The public key is $(n, e) = (221, 5)$. The private key is $(p, q, d) = (13, 17, 77)$.

   B) For Bob, $s \equiv x^d \equiv 10^{77} \equiv 192^{11} \equiv 192^3 * 192^4 * 192^4 \equiv 142 * 81 * 81 \equiv 147 \pmod{221}$

   For Alice $s^e \equiv 147^5 \equiv 147 * 147^4 \equiv 147 * 191 \equiv 10 \pmod{221}$, which is the same as x.

4. *(1 point)* Solve Problem 8.5 (p235 in Understanding Cryptography).

   Answer: For $p = 467$ and $\alpha = 2$,

   1) Public keys are $A \equiv 2^a \equiv 2^3 \equiv 8 \pmod{467}$, and $B \equiv 2^b \equiv 2^5 \equiv 32 \pmod{467}$.

   For Alice, $k_{AB} \equiv B^a \equiv 32^3 \equiv 78 \pmod{467}$.

   For Bob, $k_{AB} \equiv A^b \equiv 8^5 \equiv 78 \pmod{467}$.

   2) Public keys are $A \equiv 2^a \equiv 2^{400} \equiv 161^{20} \equiv 123^5 \equiv 123 * 134 \equiv 137 \pmod{467}$, and $B \equiv 2^b \equiv 2^{134} \equiv 161^6 * 39 \equiv 169 * 169 * 39 \equiv 84 \pmod{467}$.

   For Alice, $k_{AB} \equiv B^a \equiv 84^{400} \equiv 266^{100} \equiv 147^{25} \equiv 147 * 251^6 \equiv 147 * 164 * 164 \equiv 90 \pmod{467}$.

   For Bob, $k_{AB} \equiv A^b \equiv 137^{134} \equiv 89^{67} \equiv 89 * 449^{33} \equiv 266 * 324^{16} \equiv 266 * 461^4 \equiv 90 \pmod{467}$.

   3) Public keys are $A \equiv 2^a \equiv 2^{228} \equiv 16^{57} \equiv 52^7 * 16 \equiv 369^3 * 365 \equiv 394 \pmod{467}$, and $B \equiv 2^b \equiv 2^{57} \equiv 256^7 * 2 \equiv 156^3 * 45 \equiv 313 \pmod{467}$.

   For Alice, $k_{AB} \equiv B^a \equiv 313^{228} \equiv 394^{57} \equiv 374^7 * 394 \equiv 206 \pmod{467}$.

   For Bob, $k_{AB} \equiv A^b \equiv 394^{57} \equiv 374^7 * 394 \equiv 206 \pmod{467}$.

5. *(1 point)* Solve Problem 13.11 (p355 in Understanding Cryptography).

   Answer:

   From Q5.3 we know $A = 394$ and $B = 313$. Then $O \equiv 2^o \equiv 2^{16} \equiv 156 \pmod{467}$.

   For Oscar, $k_{AO} \equiv A^o \equiv 394^{16} \equiv 375^2 \equiv 243 \pmod{467}$, and $k_{BO} \equiv B^o \equiv 313^{16} \equiv 394^4 \equiv 438 \pmod{467}$.

   For Alice, $k_{AO} \equiv O^a \equiv 156^{228} \equiv 369^{57} \equiv 160^7 * 369 \equiv 243 \pmod{467}$.

   For Bob, $k_{BO} \equiv O^b \equiv 156^{57} \equiv 264^7 * 156 \equiv 438 \pmod{467}$.

Bonus. *(1 point)* Solve Problem 7.13 (p202 in Understanding Cryptography).

Answer:

- If applied letter by letter, RSA can be treated as a substitution cipher With n being small, Oscar can precompute a table listing each plaintext and its corresponding ciphertext which is essentially the key to the substitution cipher. Therefore Oscar can decrypt any message.
- As above, part of the table could be: $y_A \equiv A^e \equiv 65^{11} \equiv 3288 \pmod{3763}$, $y_B \equiv B^e \equiv 66^{11} \equiv 705 \pmod{3763}$, etc. In particular, $y_I = 1125$, $y_M = 333$, $y_N = 3368$, $y_O = 2929$, $y_P = 3696$, $y_S = 2514$. Therefore the message is SIMPSONS.
- OAEP padding would require to use a much larger n, which makes the above attack impractical.