Homework 1

CSIT 5730

Written Assignment

Some questions in this assignment come from the textbook: `Information Security Principles and Practice`. Nevertheless, you don't need to read the textbook in order to solve the questions.

This assignment has in total 100 points. That will count 4% of your final grade.

1. (6pt) Find the plaintext and the key, given the ciphertext: `Kdssb Krolgdbv`.[1]

   (a) (**answer**): the shift is 3 (or, equivalently, -23), and the plaintext is "Happy Holidays."

2. (8pt) Answer the questions about one-time pad using the letter encodings in Table 1.

letter	d	c	b	l	i	z	u	y
binary	000	001	010	011	100	101	110	111

Table 1: Alphabet encoding.

   (a) (4pt) Use the key "`clzyu`" to encrypt the plaintext "`dcliz`". What is the ciphertext? Explain briefly.

   (b) (4pt) What is the secret key that is used to encrypt "`yibc`" to "`zuld`". Explain briefly.

   (a) (**answer**): According to Table 1, the binary encodings of the key and plaintext are `001 011 101 111 110` and `000 001 011 100 101`, respectively. XOR them to get the ciphertext binary `001 010 110 011 011`, which translates to "`cbull`".

   (b) (**answer**): Translate the words to `111 100 010 001` and `101 110 011 000`, respectively, then XOR them to get the key. The key is `010 010 001 001` ("`bbcc`").

3. (10pt) Suppose that Alice's RSA public key is (N, e) = (323,5) and her private key is d = 29.

   (a) (4pt) If Bob encrypts the message $M = 121$ using Alice's public key, what is the ciphertext C? Show that Alice can decrypt C to obtain M.

   (b) (6pt) Let S be the result when Alice digitally signs the message $M = 2$. What is S? If Bob receives M and S, explain the process Bob will use to verify the signature and show that in this particular case, the signature verification succeeds.

   (a) (**answer**): to encrypt: $121^5 = 49 \bmod 323$. To decrypt: $49^{29} = 121 \bmod 323$.

[1] Hint: The key is a shift of the alphabet.

(b) (**answer**): The signed result is $S = M^d \bmod N = 2^{29} \bmod 323 = 15$. To verify the signature, Bob computes $S^5 \bmod N$ and the signature is verified if the result matches the received value M. In this case, $15^5 = 2 \bmod 323$. Assuming Bob receives the sent message $M = 2$, the signature is verified.

4. (10pt) For A5/1 cipher, suppose that, after a particular step, the values in the registers are

$$X = (x_0, x_1, ..., x_{18}) = (1110101000101000101)$$
$$Y = (y_0, y_1, ..., y_{21}) = (10000100111011001110 11)$$
$$Z = (z_0, z_1, ..., z_{22}) = (10101001011010011010000)$$

(a) (4pt) What is the next 2 keystream bits?

(b) (6pt) What are the contents of X,Y and Z, respectively, after these 2 bits have been generated?

(a) (**answer**) The next 2 keystream bits are 0 and 1.
Explanation:
Fist step: $t_Y = y_{20} \oplus y_{21} = 1 \oplus 1 = 0$,
$t_Z = z_7 \oplus z_{20} \oplus z_{21} \oplus z_{22} = 1 \oplus 0 \oplus 0 \oplus 0 = 1$,
So after step:
$X = (1110101000101000101)$
$Y = (0100001001110110011101)$
$Z = (1101010010110100 1101000)$
Keystream bit $= 1 \oplus 1 \oplus 0 = 0$
Second step: $m = maj(x_8, y_{10}, z_{10}) = maj(0, 1, 1) = 1$. So X does not step, Y and Z step.
$t_Y = y_{20} \oplus y_{21} = 0 \oplus 1 = 1$
$t_Z = z_7 \oplus z_{20} \oplus z_{21} \oplus z_{22} = 0 \oplus 0 \oplus 0 \oplus 0 = 0$
So after step:
$X = (1110101000101000101)$
$Y = (1010000100111011001110)$
$Z = (0110101001011010011 0100)$
Keystream bit $= 1 \oplus 0 \oplus 0 = 1$

(b) (**answer**) after step:
$X = (1110101000101000101)$
$Y = (1010000100111011001110)$
$Z = (0110101001011010011 0100)$

5. (8pt) This problem deals with the A5/1 cipher.

(a) (2pt) On average, how often does the Y register step? And why? Please explain your answer.

(b) (2pt) On average, how often do all three registers step? Please explain your answer.

(c) (2pt) On average, how often do at least two registers step? Please explain your answer.

(d) (2pt) On average, how often does no register step? Please explain your answer.

(a) (**answer**): This register steps exactly 75% of the time. Given three bits from three registers, there are 6 out of 8 possibilities that bit from Y match the majority voting output and therefore Y got steps.

(b) (**answer**): All 3 registers step when all three "step bits" agree, that is, in the 000 and 111 case, which occur $2/8 = 25\%$ if the time.

(c) (**answer**): Two registers step in all cases, so 100% of the time.

(d) (**answer**): Never, since it is not possible that no register will be in the majority; there are 3 registers, so a majority consists of 2 or more.

6. (16pt) Consider a Feistel cipher with three rounds. We want to encrypt the plaintext $P = (L_0, R_0)$ and the corresponding ciphertext is $C = (L_3, R_3)$. What is the ciphertext C, in terms of L_0, R_0, and the subkey K_i, for each of the following round functions?

   (a) (2pt) $F(R_i, K_i) = D$ (D is some constant)

   (b) (4pt) $F(R_i, K_i) = K_i$

   (c) (6pt) $F(R_i, K_i) = R_i \oplus K_i$

   (d) (4pt) Is it reasonable to use the round function $F(R_i, K_i) = L_i \oplus K_i$? Breif explain why and why not.

   (a) (**answer**) $C = (R_0 \oplus D, L_0)$

   (b) (**answer**): $C = (R_0 \oplus K_1, L_0 \oplus K_0 \oplus K_2)$

   (c) (**answer**): $C = (L_0 \oplus K_0 \oplus K_1, R_0 \oplus K_1 \oplus K_2)$

   (d) (**answer**): No, This will lose the original information both L_i and R_i about the original plaintext.

   Note: swapping the two halves of the output plaintext is also accepted because it's the scheme from the lecture slides.

7. (8pt) Alice has four blocks of plaintext, P_0, P_1, P_2, P_3, which she encrypts using CBC mode to obtain C_0, C_1, C_2, C_3. She then sends the IV and ciphertext to Bob. Upon receiving the ciphertext, Bob plans to verify the integrity as follows. He will first decrypt to obtain the putative plaintext, and then he will re-encrypt this plaintext using CBC mode and the received IV. If he obtains the same C_3 as the final ciphertext block, he will trust the integrity of the plaintext.

(a) (4pt) Suppose that an attacker changes C_2 to X, leaving all other blocks and the IV unchanged. Will Bob detect that the data lacks integrity? Explain briefly.

(b) (4pt) Alice encrypts four blocks of plaintext, P'_0, P'_1, P'_2, P'_3, to obtain C'_0, C'_1, C'_2, C'_3. If $P'_0 = P_0$ and the IV remain unchanged, how many blocks in C_0, C_1, C_2, C_3 and C'_0, C'_1, C'_2, C'_3 are equal? Explain briefly.

(a) (**answer**): No, since Bob is just decrypting and then re-encrypting with the same key, so he will get what he started with.

(b) (**answer**): $C_0 = C'_0$, because the IV remain unchanged.

8. (8pt) Suppose that Bob proposes the following variant of RSA. He first chooses N, then he finds three encryption exponents e_0, e_1 and e_2 and the corresponding decryption exponents d_0, d_1 and d_2. He asks Alice to encrypt her message M to him by first computing $C_0 = M^{e_0} \pmod N$, $C_1 = C_0^{e_1} \pmod N$, then encrypting C_1 to obtain the ciphertext, $C_2 = C_1^{e_2} \pmod N$. Alice then sends C_2 to Bob.

   (a) (4pt) Does this multiple encryption increase the security of RSA?

   (b) (4pt) Why or why not?

   (a) (**answer**): No.

   (b) (**answer**): This process is equivalent to the single encryption with $e = e_0 * e_1 * e_2$.

9. (6pt) Suppose that Trudy wants to establish a single Diffie-Hellman value, $g^{abt} \bmod p$, that she, Alice, and Bob all share. Does the attack illustrated in Figure. 1 succeed? Justify your answer.

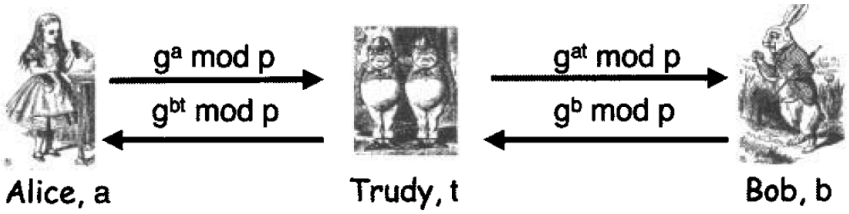

Figure 1: Main-in-the-Middle Attack

   (a) (**answer**) No. Trudy has no way to determine the secret value $g^{abt} \bmod p$ that Alice and Bob will share. It is equivalent to solving a discrete log problem.

10. (10pt) This question is about S-box and block cipher. Considering the following S-box, which maps 3 bits $(x_0x_1x_2)$ to 2 bits (y_0y_1). As shown in the S-box, x_0 forms the row index while x_1x_2 form the column index. Please answer questions:

2^*x_0	x_1x_2 00	01	10	11
0	01	00	11	10
1	11	10	00	01

(a) (2pt) Analyze the probability that $y_1 = x_0$;

(b) (2pt) Analyze the probability that $y_1 = x_1$;

(c) (2pt) Analyze the probability that $y_0 = x_1 \oplus x_2$;

(d) (4pt) Suppose that we use counter mode encryption to encrypt according to the formula: $C_i = P_i \oplus E(IV, K)$, where E is the encryption function of a secure block cipher. Is this secure? Why or why not? If not, give a secure formula.

(a) (**answer**): $y_1 = x_0$ happens when $x_0x_1x_2$ in $\{100, 001, 011, 111\}$. The probability is 4/8.

(b) (**answer**): $y_1 = x_1$ happens when $x_0x_1x_2$ in $\{001, 101, 010, 111\}$. The probability is 4/8.

(c) (**answer**): $y_0 = x_1 \oplus x_2$ happens when $x_0x_1x_2$ in $\{000, 101, 010, 111\}$. The probability is 4/8.

(d) (**answer**): No. The same IV will be used for all blocks, which will lead to the same ciphertext for the same plaintext. Secure formula: $C_i = P_i \oplus E(IV + i, K)$.

11. (10pt) To speed up RSA, it is possible to choose $e = 3$ for all users. However, this creates the possibility of a cube root attack.

(a) (3pt) Briefly explain the cube root attack. You can Google it but please use your own language to describe.

(b) (3pt) For $(N, e) = (33, 3)$ and $d = 7$, show that the cube root attack works when $M = 3$ but not not when $M = 4$.

(c) (4pt) Propose a strategy that uses message padding to prevent the cube root attack, assuming $e = 3$ must be used.

(a) (**answer**) If $M^3 < N$, then the $\mod N$ operation has no effect, so Trudy can simply take the usual cube root of the ciphertext to decrypt.

(b) (**answer**) Since $3^3 = 27 < 33$, Trudy can take the cube root to obtain M, but $4^3 = 64 = 31 \mod 33$, so Trudy cannot simply take the cube root.

(c) (**answer**) The most straightforward solution is to pad with random bits, making sure that a sufficiently high order is set to 1 so that when the padding is included, $M > N^{1/3}$, regardless of the actual message. (reasonable result gets full grade)

Submission Instructions

All submissions should be done through the Canvas system. You should submit a pdf document with your answers for each question.

It is important to name your files correctly. Please check out the late submission policies on the course website in case you didn't attend the first lecture.