COSC362 Data and Network Security Assignment

Name: Jordan Pyott
ID: 87433186

Question One:

Cryptosystems based on discrete logarithms (see later during Term 4) often make use of a prime number p and a generator g of the integers modulo p, that is $\mathbb{Z}_p^*$.

Show that when $p = 17$, the value 2 is not a generator but that 3 is a generator.

Answers:

Show that 2 is not a generator: $[2] = \{0, 1, 4, 9, 16, 8, 2, 15, 13, 13, 15, 2, 8, 16, 9, 4, 1, 0, 1, 4\}$

Show that 3 is a generator: $[3] = \{0, 1, 8, 10, 13, 6, 12, 3, 2, 15, 14, 5, 11, 4, 7, 9, 16, 0, 1, 8\}$

When $g = 3$ the generator can produce all values within the set $\mathbb{Z}_p$ and is there for a generator of $\mathbb{Z}_p$.

Question Two:

Suppose that a certain encryption algorithm uses a secret key of 64 bits and that an attacker has the ability to test all possible keys within one year.

a. Estimate how many keys per second the attacker can test. You may use the approximation that there are 225 seconds in a year. (1 mark)

b. Given a particular ciphertext to test, how could this attacker know when the correct key is found? (1 mark)

Answers:

a. $\frac{2^{64}}{2^{25}} = 549755813888$, therefore the attacker would have to process 549755813888 keys per second.

b. The attacker could verify if the key is correct by using the decrypt function of the cipher and checking if the output is readable or not (one method of automating this is to use a wordlist).

Question Three:

a. What is the equation for decryption of ciphertext block C_t to obtain P_t ? (1 mark)

b. If one bit is flipped in ciphertext block C_t , how many bits are changed in the decrypted plaintext? Explain your answer. (1.5 marks)

c. Define a Message Authentication Code (MAC) so that the last complete block of the message encrypted with CTR is the MAC tag. Would this be a good MAC? Explain your answer. (1.5 marks)

Answers:

a. $p_t = O_t \oplus C_t$

b. Due to the nature of CTR and the XOR operation, if C_t has a flipped bit, because CTR has no chaining, and the XOR operation is only applied to a single bit, the plainttext will also contain a single flipped bit in the same location as the ciphertext.

c. $C_t = O_t \oplus P_t, T = C_n, T_t = N||t, O_t = E(T_t, K)$

Note that this is a poor choice of MAC, a good mac would check the integrity of all blocks, however effectively what we are doing by pushing the last block to hold the MAC Tag, we are not checking the integrity of all blocks except the last block, this is because CTR does not have block chaining. This method would be fine if we were using CBC.

Question Four:

a. If one bit is flipped in message block $P2$ and the whole message is re-encrypted, how different are the new ciphertext blocks $C10, C20, C30, C40$ in comparison with the original ciphertext blocks $C1, C2, C3, C4$? (1.5 marks)

b. If one bit is flipped in ciphertext block $C2$ and the whole message is decrypted, how different are the new decrypted plaintext blocks $P01, P02, P03, P04$ in comparison with the original plaintext blocks $P1, P2, P3, P4$? (1.5 marks)

Answers:

a. If a single bit is flipped in P_2 then C_2', C_3', C_4' will all be completely garbled as the bit flip occurred before the block cipher encryption and the error will be carried to C_3', C_4' due to the XOR operation and this is calculated before the block cipher encryption. This means that:

$$C_1' = C_1$$

$$C_2' \neq C_2$$

$$C_3' \neq C_3$$

$$C_4' \neq C_4$$

b. If a single bit is flipped in C_2, then P_2' is now garbled, due to the block cipher decryption. P_3' will have a single bit flipped because at the same local as C_2 because in CBC the original ciphertext is XOR'd before going into the block cipher decryption and C_3 does not contain any errors. Because the cipher text C_3 does not contain any errors, and neither does C_4, they will be XOR'd to produce plaintext P_4' which will have errors or flipped bits, therefore:

$$P_1' = P_1$$

$$P_2' \neq P_2$$

$$P_3' \neq P_3$$

$$P_4' = P_4$$