Liam Donohoe
RCSID: donohl
RIN: 661634267

Crypto HW2.b

1. Users A and B use the Diffie-Hellman key exchange technique with a common prime q = 71 and a primitive root α = 7.
    a. A's public key $Y_A = 7^5 \bmod 71 = 51$
    b. B's public key $Y_B = 7^{12} \bmod 71 = 4$
    c. The shared session key is $51^{12} \bmod 71 = 30 = 4^5 \bmod 71$.
    d. If the participants were to send $x^a \bmod q$ instead of $a^x \bmod q$, then they would not necessarily obtain the same session key. Diffie-Hellman works because the alpha value is chosen from the primitive roots of the prime. Using this as the power instead would not guarantee that both parties would obtain the same key.
2. A network resource X is prepared to sign a message by appending the appropriate 64- bit hash code and encrypting that hash code with X's private key as described in class (also in the textbook, Page 330.
    a. With hash codes, there is a slight chance that two signatures can calculate to be the same value, resulting in a hash table collision. This is called the Birthday Attack, where by using a collision, the attacker can send a fraudulent message, and obtains a valid signature on it. This would allow them to send a fake message, and remain undetected. They could generate this message using a set of $2^{m/2}$ valid messages, and a separate set of fraudulent messages of the same size. They can then compare between these two sets, and find hash collisions between the pairs, telling them what fraudulent messages can be used to impersonate which valid messages.
    b. The attacker would need to generate $2^{m/2} * 2^{m/2} = 2^m$ pairs.
    c. At this rate, it would take $2^{64} / 2^{20} = 2^{44}$ seconds.
    d. With m = 128 bits, the memory usage is now 2^{128}, and the time is $2^{128}/2^{20} = 2^{108}$ seconds.
3. Use Trapdoor Oneway Function with following secrets as described in lecture notes to encrypt plaintext P = '0101 0111'. Decrypt the resulting ciphertext to obtain the plaintext P back. Show each step to get full credit. S = {5, 9, 21, 45, 103, 215, 450, 946}, a = 1019, p = 1999
    a. First, Generate the public key S * 1019 mod 1999 = {1097, 1175, 1409, 1877, 1009, 1194, 779, 456}
    b. Using this key to encrypt '0101 0111' we get, C = 1175 + 1877 + 1194 + 779 + 456 = 5481.
    c. Now we solve $a^{-1} \bmod 1999$. This is equivalent to a = 1 mod 1999.
    We can find that 1 = (1999) 209 - (1019) 410. This is equivalent to 1 mod 1999 = (1999)209 - (1019)410 mod 1999. Reducing this, we get 1 mod 1999 = (1019) -410 mod 1999. Therefore, $a^{-1} = -410 \bmod 1999 = 1589 \bmod 1999$.
    To decrypt the ciphertext 5481, we can use $C * a^{-1} = 5481 * 1589 \bmod 1999 = 1665$.
    We then reverse the subset sum to get 1665 = 946 + 450 + 215 + 45 + 9. These elements correspond to the elements of S giving us our plaintext P = '0101 0111'.