Homework 3 – CS 458

Christopher Morcom

13 October 2018

Problem 1:
We now consider the relation between passwords and key size. For this purpose we consider a cryptosystem where the user enters a key in the form of a password.

a. **Assume a password consisting of 8 letters, where each letter is encoded by the ASCII scheme (7 bits per character, i.e., 128 possible characters). What is the size of the key space which can be constructed by such passwords?**

   $\text{key space size} = \text{no. possible passwords} = 128^8 = 2^{56}$
   (This assumes each character is equally likely to be chosen with repetition.)

b. **What is the corresponding key length in bits?**

   $\text{key length (bits)} = \text{bits per char} * \text{ no. chars} = 7 * 8 = 56 \text{ bits}$

c. **Assume that most users use only the 26 lowercase letters from the alphabet instead of the full 7 bits of the ASCII-encoding. What is the corresponding key length in bits in this case?**

   Given 26 characters, there are $\lceil \log_2 26 \rceil = 5\ bits/char$ so:
   $keylength(bits) = 8 * 5 = 40bits$

Problem 2:
There are elements in Z_4 and Z_6 without a multiplicative inverse. Which elements are these? Why does a multiplicative inverse exist for all nonzero elements in Z_5?

Note that for any $x \in Z_n$, if the greatest common denominator (GCD) is 1 (they are co-prime numbers), then they have a multiplicative inverse, otherwise no inverse exists.

for Z_4, 2 is prime, but not co-prime with 4 so no multiplicative inverse exists.

for Z_6, 2,3,4 are not co-prime with 6 so no multiplicative inverse exists.

for Z_5, 1,2,3,4 are co-prime with 5, so a multiplicative inverse exists for all nonzero elements in Z_5.

Problem 3:
What is the multiplicative inverse of 5 in Z_{11}, Z_{12}, and Z_{13}?

Note the multiplicative inverse modulo formula for Z_n:
$$(a * x) \bmod n = 1$$
Where x is the multiplicative inverse of a.

For Z_{11}	$(5x) \bmod 11 = 1$ $x = 9$
For Z_{12}	$(5x) \bmod 12 = 1$ $x = 5$
For Z_{13}	$(5x) \bmod 13 = 1$ $x = 8$

Problem 4:
Compute the following values: $\Phi(100)$, $\Phi(40)$, $\Phi(101)$.

$\Phi(100) = $ count(GCD(100,n) for all n in Z_{100}) $\Phi(100) = 40$
$\Phi(40) = $ count(GCD(40,n) for all n in Z_{40}) $\Phi(40) = 16$
$\Phi(101) = $count(GCD(101,n) for all n in Z_{101}) $\Phi(101) = 100$ (for prime numbers $\Phi(n) = n - 1$)

Problem 5:

One important property which makes DES secure is that the *S-boxes* are nonlinear. How would you **verify** (not prove of course) the non-linearity of *S-box 1* of DES using the following input pairs

1. x_1 = *000000*, x_2 = *000001*
2. x_1 = *111111*, x_2 = *100000*

S-Box 1 of DES

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

We can verify the non-linearity of S-Box 1 of DES by checking the input pairs and comparing the $\Delta y/\Delta x$ for the input pairs.

For pair 1, $\Delta y/\Delta x = -14/1 = -14$
For pair 2, $\Delta y/\Delta x = -9/-31 = 9/31$
Since both $\Delta y/\Delta x$ are not equal, we can say that the S-Box 1 of DES is non linear. We can further verify this by checking all input pairs of the S-Box by column.

Problem 6:
Explain the self-healing property of cipher block chaining mode?

Say we have a multi-block cipher chain. Let block n be corrupted. During decryption, block n would be converted into a trash output. When we XOR block N+1 with block n, we can then operate n XOR n to get the error and replace it everywhere so that when we decrypt block n+2, we can see the self-healing property as the corruption that transferred form block 1 to block n+1 becomes omitted as the block n+2 is being decrypted.

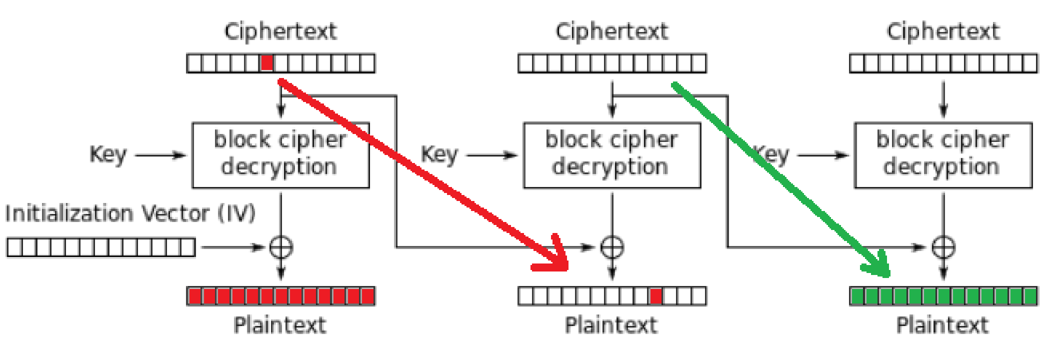

Image source: https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

Problem 7:
Perform encryption using the RSA algorithm, for the following:

1. p = 3, q = 11, e = 7, M = 5

$n = 3 \times 11 = 33$
$\varphi(pq) = (3-1)(11-1) = 20$
$(de) mod\ 20 = 1$
de = 20+1= 21 such that e is a number where gcd(20,e)=1
e=7, d = 3 (trial and error)
$\mathrm{C} = \mathrm{M}^{\mathrm{e}} mod\ n = 5^7 mod\ 33 = 14$

2. p = 5, q = 17, e = 3, M = 9

$n = 5 * 17 = 85$
$\varphi(pq) = (5-1)(17-1) = 64$
$(de) mod\ 64 = 1$
de = 65 such that e is a number where gcd(64,e)=1
e=13, d = 5 (trial and error)
$C = M^e mod\ n = 9^{13} mod\ 64 = 41$

Problem 8:
Perform decryption using the RSA algorithm, for p = 11, q = 13, e = 11; C = 106

$M = C^d\ mod\ n = M = 106^d mod(11 * 13)$
$demod\varphi(pq) = 1 = 11(d)mod120$
d = 11
$M = 106^{11} mod(143)$
M = 7

Problem 9:
In a public-key system using RSA, you intercept the ciphertext C =10 sent to a user whose public key is e=5 , n=35 . What is the plaintext M ?

$M = C^d\ mod\ n = M = 10^d mod(35)$
p = 5, q = 7
$de\ mod\varphi(pq) = 1 = 5(d)mod24$
d = 5
$M = 10^5 mod(35)$
M = 5

Problem 10:

Alice and Bob use the Diffie-Hellman key exchange technique with a common prime $p = 71$ and a primitive root $\alpha = 7$.

1. If Alice has private key $k_{pr,A} = 5$, what is Alice's public key $k_{pub,A}$?
2. If Bob has private key $k_{pr,B} = 12$, what is Bob's public key $k_{pub,B}$?
3. What is the shared secret key?

Note: $K_{pub,A} = \propto^{K_{pr,A}} \; mod \; p$

Note: $SharedKey(A) = K_{pub,B}{}^{K_{pr,A}} mod \; p$

$SharedKey(B) = K_{pub,A}{}^{K_{pr,B}} modp$

1. $K_{pub,A} = 7^5 mod \; 71 = 51$
2. $K_{pub,B} = 7^{12} mod \; 71 = 4$
3. $SharedKey(A) = 4^5 mod \; 71 = 30 = SharedKey(B) = 51^{12} mod \; 71 = 30$
   $Shared \; Key = 30$

Comment Summary