Problem Set 2

Sunday, March 1, 2020 12:08 PM

Problem #1 - Relationship between passwords & Key size

a) Assume password is 8 letters (ASCII scheme). What is the size of the key space which can be constructed by such passwords?

Password size: 8 — — — — — — —

↓

7bit per letter → (0,1) → $2^7 = 128$ characters

Since there is no restriction on repeating characters, then each letter can be of the any 128 characters.

∴ $128^8 = \boxed{2^{56}}$

b) What is the corresponding key length?

The key length leads to the total amount of possible passwords.

∴ since 2^{56} was total possible passwords.

The key length is 56 $\log_2(2^{56}) = 56$

c) Assume most users use only the lowercase letters. What is the corresponding key length?

If only lowercase letters are used then the possible # of passwords is reduced from $128^8 = 2^{56}$ to 26^8.

The key length would then be

$\log_2(26^8) \approx \boxed{37.603}$

Problem #2 - DES & S-Boxes

An important property of DES that makes it secure is that the S-boxes are non-linear. How would you verify the non-linearity of S-box 1 of DES with the following?

1) $X_1 =$ 000000, $X_2 =$ 000001

A linear function has the following 2 properties:

- Additivity: $f(x+y) = f(x) + f(y)$
- Homogeneity of degree 1: $f(a \cdot x) = a \cdot f(x)$ for all a

Thus, to verify it is non-linear we must test at least one

$S_1(X_1 + X_2) \stackrel{?}{=} S_1(X_1) + S_1(X_2)$

$S_1(000000) = 14$ (0 row, 7 col) $\quad S_2(000001) = 0$ (1 row, 0 col)

00 = 0 $\qquad$ 01 = 1

$S_1(000000 + 000001) = S_1(000001) = 0$

∴ $\boxed{S_1(X_1 + X_2) \neq S(X_1) + S(X_2)}$

2) $x_2 = 111111$, $x_2 = 100000$

$S_1(x_1 + x_2) \stackrel{?}{=} S_1(x_1) + S_1(x_2)$

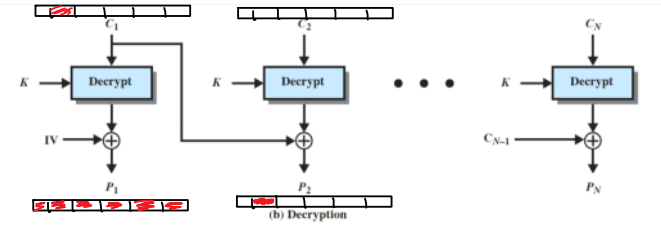
$S_1(111111) = 13$ (15 col, 3 row, 11 = 3) $\quad S_1(100000) = 4$ (0 col, 2 row, 10 = 2)

$S_1(111111 + 100000) = S_1(\emptyset 011111) = 13 \neq 17$ (15, 3 row)

$\therefore \boxed{S_1(x_1 + x_2) \neq S(x_1) + S_2(x_2)}$

Problem #3 - Self-Healing

Taking a look into the decryption process of CBC:



If C_1 contains a corrupted bit, then P_1 will be fully affected by the corruption.

Since C_1 is also used to decrypt C_2, then a P_2 will be partially corrupted.

Because of this, only 2 blocks at most will be affected by the corruption.

Problem #4 - RSA Alg. Encryption

Perform encryption using RSA alg. on the following,

1) $p = 3$, $q = 11$, $e = 7$, $M = 5$

$N = pq = (3)(11) = 33$

Encrypt:

$C = M^e \bmod n = 5^7 \bmod 33 = \boxed{14}$

2) $p = 5$, $q = 17$, $e = 3$, $M = 9$

$N = p \cdot q = (5)(17) = 85$

$\vdots$

$C = M^e \bmod N = (9)^3 \bmod 85 = \boxed{49}$

Problem #5 - RSA Alg. Decryption

Perform decryption using RSA for:
$p = 11$, $q = 13$, $e = 11$; $C = 106$

$N = p \cdot q = (11)(13) = 143$; $\varphi(n) = (p-1)(q-1) = (10)(12) = 120$

$\gcd(\varphi(n), e) = \gcd(120, 11) = 1$

Because e & d are inverse:
$ed \bmod \varphi(n) = 1 = 11d \bmod 120$
so $d = 11$

Decrypt:
$M = C^d \bmod N = (106)^{11} \bmod 143 = \boxed{7}$

Problem #6 - RSA Intercept

You intercept the ciphertext $C = 10$ sent to a user whose public key is $e = 5$, $n = 35$. What is plaintext M?

$N = 35$, $\varphi(n) = (6)(4) = 24$
$7 \quad 5$
$\gcd(\varphi(n), e) = \gcd(24, 5) = 1$

Because e & d are inverse
$e \cdot d \bmod \varphi(n) = 1 = 5d \bmod 24$
$d = 5$

Decrypt:
$M = C^d \bmod N = (10)^5 \bmod 35 = \boxed{5}$

Problem #7 - Diff-Hellman

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

1) If Alice has a private key $K_{pr,A} = 5$, what is Alice's public key $K_{pub,A}$?

$K_{pub,A} = \alpha^a \bmod p = (7)^5 \bmod 71 = \boxed{51}$ A

2) If Bob has private key $K_{pr,B} = 12$, what is Bob's public key $K_{pub,B}$?

$K_{pub,B} = \alpha^b \bmod p = (7)^{12} \bmod 71 = \boxed{4}$ B

3) What is the shared key?

$K_{AB} = B^a = 4^5 \bmod 71 = \boxed{30}$ ✓

$K_{AB} = A^b = 51^{12} \bmod 71 = \boxed{30}$ ✓