CIS 3362 Final Exam - Part A (Classical Cryptography) - 25 pts Solutions

1) (5 pts) How many possible keys are there for an affine cipher for an alphabet of size 60?

Solution

The affine cipher encryption function takes the form f(x) = (ax + b) mod n, where n is the alphabet size. b can be any value in between 0 and n-1, and a must be a value in between 0 and n-1 that is relatively prime with n. There are φ(n) such values. Any valid value of a and be paired with any valid value of b, so we multiply the # of valid values of each to obtain the number of possible keys there are, which is

$60*\varphi(60) = 60*\varphi(2^2*3*5) = 60\varphi(2^2)\varphi(3)\varphi(5) = 60(2^2 - 2)(3 - 1)(5 - 1) = 60(2)(2)(4) =$ **960.**

Grading: 1 pt for 60, 3 pts for phi(60), 1 pt for multiplying

2) (10 pts) In a set of 100 bits (zeroes and ones), the index of coincidence is $\frac{19}{33}$. Let x be the number of 0s in the set and y be the number of 1s in the set. What is |x - y|?

Solution

Since there are 100 total bits y = 100 - x. the index of coincidence of the set is

$$\frac{x(x-1) + (100-x)(99-x)}{100 \times 99}$$

Set this equal to $\frac{19}{33}$ and solve for x, using the calculator for multiplications:

$$\frac{x(x-1) + (100-x)(99-x)}{100 \times 99} = \frac{19}{33}$$

$$33[x^2 - x + 9900 - 199x + x^2] = 100 \times 99 \times 19$$

$$x^2 - x + 9900 - 199x + x^2 = 5700$$

$$2x^2 - 200x + 4200 = 0$$

$$x^2 - 100x + 2100 = 0$$

$$(x - 30)(x - 70) = 0$$

Thus, x = 30 or x = 70. If x is 30, y is 70 and vice versa. Either way, |x - y| = |30-70| = **40.**

Grading: 4 pts for expression of IofC in terms of x,
1 pt for setting this expression equal to 19/33
4 pts for solving for x (can give partial)
1 pt for answering the question using either answer of x.

3) (10 pts) You are trying to find the encryption key for a Hill cipher with block size two for a regular alphabet size of 26 and know that the plaintext "TRIP" maps to the ciphertext "TJMP". Use this information to determine the ***encryption*** key. Note: The encryption key is a matrix of the form $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, where 0 ≤ a, b, c, d ≤ 25.

Solution

Here are the corresponding equations for the encryption key, noting that TRIP converts to 19, 17, 8, 15 and TJMP converts to 19, 9, 12, 15, numerically:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 19 \\ 17 \end{pmatrix} = \begin{pmatrix} 19 \\ 9 \end{pmatrix} \ mod\ 26$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 8 \\ 15 \end{pmatrix} = \begin{pmatrix} 12 \\ 15 \end{pmatrix} \ mod\ 26$$

The corresponding sets of equations, we regrouped appropriately (take first equation from both pairs and put those together and second equation from both pairs and put those together):

19a + 17b ≡ 19 mod 26
8a + 15b ≡ 12 mod 26

19c + 17d ≡ 9 mod 26
8c + 15d ≡ 15 mod 26

Multiply both sets of equations by 15 and 17 respectively and subtract, use a calculator for the arithmetic:

15*19a + 15*17b ≡ 15*19 mod 26
-17*8a + 17*15b ≡ 17*12 mod 26

149a ≡ 81 (mod 26)
19a ≡ 3 (mod 26)

15*19c + 15*17d ≡ 15*9 mod 26
-17*8c + 17*15d ≡ 17*15 mod 26

149c ≡ -120 (mod 26)
19c ≡ 10 (mod 26)

Look on the modular inverse lookup chart to find that 19^{-1} mod 26 = 11 and multiply through:

11*19a ≡ 11*3 (mod 26)
a ≡ 33 ≡ 7 (mod 26)

11*19c ≡ 11*10 (mod 26)
c ≡ 110 ≡ 6 (mod 26)

Backsubstitute for

19(7) + 17b ≡ 19 mod 26
17b ≡ -114 mod 26
17b ≡ 16 mod 26, since 17^{-1} ≡ 23 (mod 26),
23(17)b ≡ 23*16 mod 26, so **b ≡ 4 (mod 26)**

19(6) + 17d ≡ 9 mod 26
17d ≡ -105 (mod 25)
17d ≡ 25 (mod 25)
23(17)d ≡ 23*25 mod 26, so **d ≡ 3 (mod 26)**

Thus, the matrix is $\begin{pmatrix} \mathbf{7} & \mathbf{4} \\ \mathbf{6} & \mathbf{3} \end{pmatrix}$.

Grading: 4 pts for setting up 4 equations, 2 pts to get to isolating (a/b AND c/d), 4 pts for each of a, b, c, d (1 pt for each)