9/18/19 ①

Fall 2019 Crypto Exam #1 Topics

1. Shift Cipher
2. Affine Cipher
3. Extended Euclidean Algorithm
4. Substitution Cipher
5. Vigenere Cipher
6. Index of Coincidence, Mutual Index of Coincidence
7. Playfair Cipher
8. ADFGVX Cipher

Fall 2019 Crypto Exam #1 Review Questions

1) (10 pts) The ciphertext "HJCCNHZXTH" was encrypted using the shift cipher with an encryption key of 15. What is the corresponding plaintext?

2) Using an affine cipher with the encryption keys a = 9, b = 5, encrypt the plaintext "KNIGHTS"

3) If the encryption keys for the affine cipher are a = 9 and b = 5, what are the corresponding decryption keys?

4) Consider using the affine cipher on an alphabet of size 20. How many possible keys would there be? (160)

5) Find 36^{-1} mod 79

6) The ciphertext for a Vigenere cipher is "HZXKEP". If the encryption keyword is "CIPHER", what was the original plaintext?

7) Determine the index of coincidence for the following set of letters:

10 As, 25 Bs, 25 Cs, 40 Ds.

as a fraction in lowest terms.

8) Encrypt "LASTQUESTION" using the playfair cipher and the keyword "LEMONS".

① H J C C N H Z X T H

7, 9, 2, 2, 13, 7, 25, 23, 19, 7

-15 ⟶

-8, -6, -13, -13, -2, -8, 10, 8, 4, -8

18, 20, 13, 13, 24, 18, 10, 8, 4, 18

S U N N Y S K I E S

② $f(x) = (9x+5) \% 26$

"KNIGHTS"

10, 13, 8, 6, 7, 19, 18

$f(10) = 95 \% 26$ 95 − 78 = 17 R

$f(13) = (117+5) \% 26 = 122 = 18$ S

$f(8) = (72+5) \% 26 = 77 \rightarrow 25$ Z

RSZHQUL

26
52
78
104
130

13
9

③ $f(x) = (9x+5) \% 26$

Swap x, y:

$x = (9y+5) \% 26$

$9y = (x-5) \% 26$

* If alpha size ≠ 26, EEA

$3(9y) = 3(x-5) \% 26$

$y = (3x-15) \% 26$

$= \boxed{(3x+11) \% 26}$ $a=3, b=11$

(4) b could any of 20 values.
a can't share a factor with 2 or 5.
0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 5, 15 (12)

#a's = 20 − 12 = 8

total # keys = 8 × 20 = 160

$$\left\lfloor \frac{20}{2} \right\rfloor + \left\lfloor \frac{20}{5} \right\rfloor - \left\lfloor \frac{20}{2*5} \right\rfloor = 10 + 4 - 2 = 12$$

(5) $36^{-1} \bmod 79$?

$79 = 2 \times 36 + 7$

$36 = 5 \times 7 + 1$

$36 - 5 \times 7 = 1$

$36 - 5(79 - 2 \times 36) = 1$

$36 - 5 \times 79 + 10 \times 36 = 1$

$11 \times 36 - 5 \times 79 = 1$

$11 \times 36 - 5 \times 0 \equiv 1 \bmod 79$

$11 \times 36 \equiv 1 \bmod 79$

$36^{-1} \equiv 11 \bmod 79$

(6) H Z X K E O P
7, 25, 23, 11, 4, 15
− 2 8 15 7 4 17

5, 17, 8, 4, 0, −2
24

F R I D A Y

CIPHER
2, 8, 15, 7, 4, 17

9/18/19

(7) $IC = \frac{10\times9 + 25\times24 + 25\times24 + 40\times39}{100\times99}$

$= \frac{90 + 600 + 600 + 1560}{100\times99}$

$= \frac{2850}{100\times99} = \frac{57}{2\times99} = \boxed{\frac{19}{66}}$

50 | 2850 (57)
250
350

10 + 25 + 25
40 50 50
50

39 × 4 = 156

1560 + 1200 + 90 = 2850

8) Playfair "LASTQUESTION" LEMONS

L	E	M	O	N
S	A	B	C	D
F	G	H	I/J	K
P	Q	R	T	U
V	W	X	Y	Z

LA → ES
ST → CP
QU → RP
ES → LA
TI → YT
ON → NL

ESCPRPLAYTNL

9/18/19 (5)

$61^{-1} \bmod 266$

$266 = 4 \times 61 + 22$

$61 = 2 \times 22 + 17$

$22 = 1 \times 17 + 5$

$17 = 3 \times 5 + 2$

$5 = 2 \times 2 + 1$

$5 - 2 \times 2 = 1$

$5 - 2(17 - 3 \times 5) = 1$

$5 - 2 \times 17 + 6 \times 5 = 1$

$7 \times 5 - 2 \times 17 = 1$

$7(22 - 17) - 2 \times 17 = 1$

$7 \times 22 - 7 \times 17 - 2 \times 17 = 1$

$7 \times 22 - 9 \times 17 = 1$

$7 \times 22 - 9(61 - 2 \times 22) = 1$

$7 \times 22 - 9 \times 61 + 18 \times 22 = 1$

$25 \times 22 - 9 \times 61 = 1$

$25(266 - 4 \times 61) - 9 \times 61 = 1$

$25 \times 266 - 100 \times 61 - 9 \times 61 = 1$

$25 \times 266 - 109 \times 61 = 1$

$25 \times 0 - 109 \times 61 \equiv 1 \bmod 266$

$61^{-1} \equiv -109 \equiv \boxed{157 \bmod 266}$

$266 - 109 = 157$

$61 \times 4 = 244$

$61 - 44$