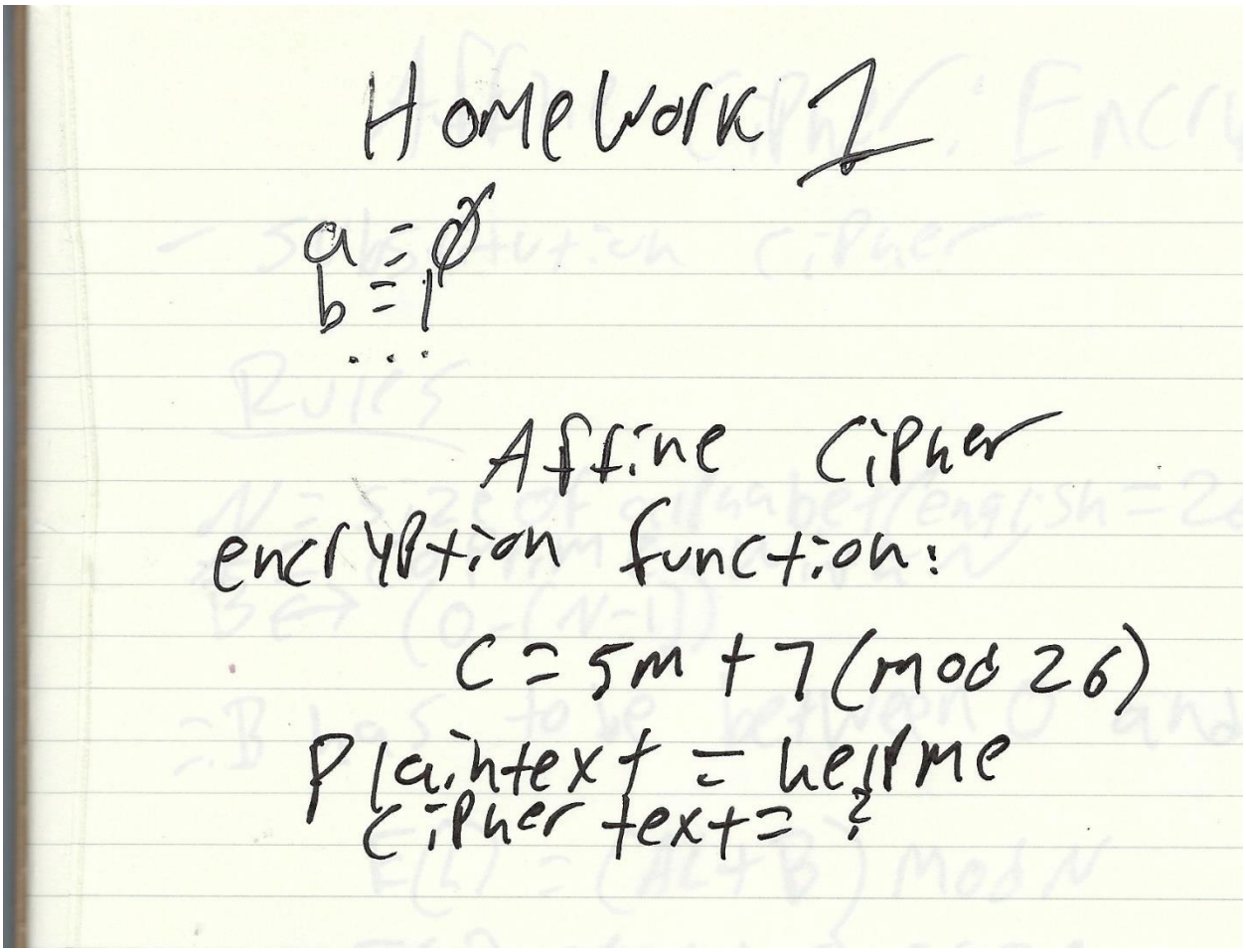
HOMEWORK 1

ROBIN WARD

COMP 7376

2/12/2020

1. 
Homework 2
a = 9
b = 1
...
Affine Cipher
encryption function:
C = 5m + 7 (mod 26)
Plaintext = hellme
Cipher text = ?

Affine Cipher: Encryption

- substitution cipher

Rules

N = size of alphabet (english = 26)
A = coprime with N
B → (0-(N-1))
∴ B has to be between 0 and 25

$$E(L) = (AL + B) \bmod N$$

$$E(L) = (3L + 5) \% 26$$
$$E(2) = (3 \times 2 + 5) \% 26$$
$$E(2) = 11 \% 26$$
$$E(2) = 11$$

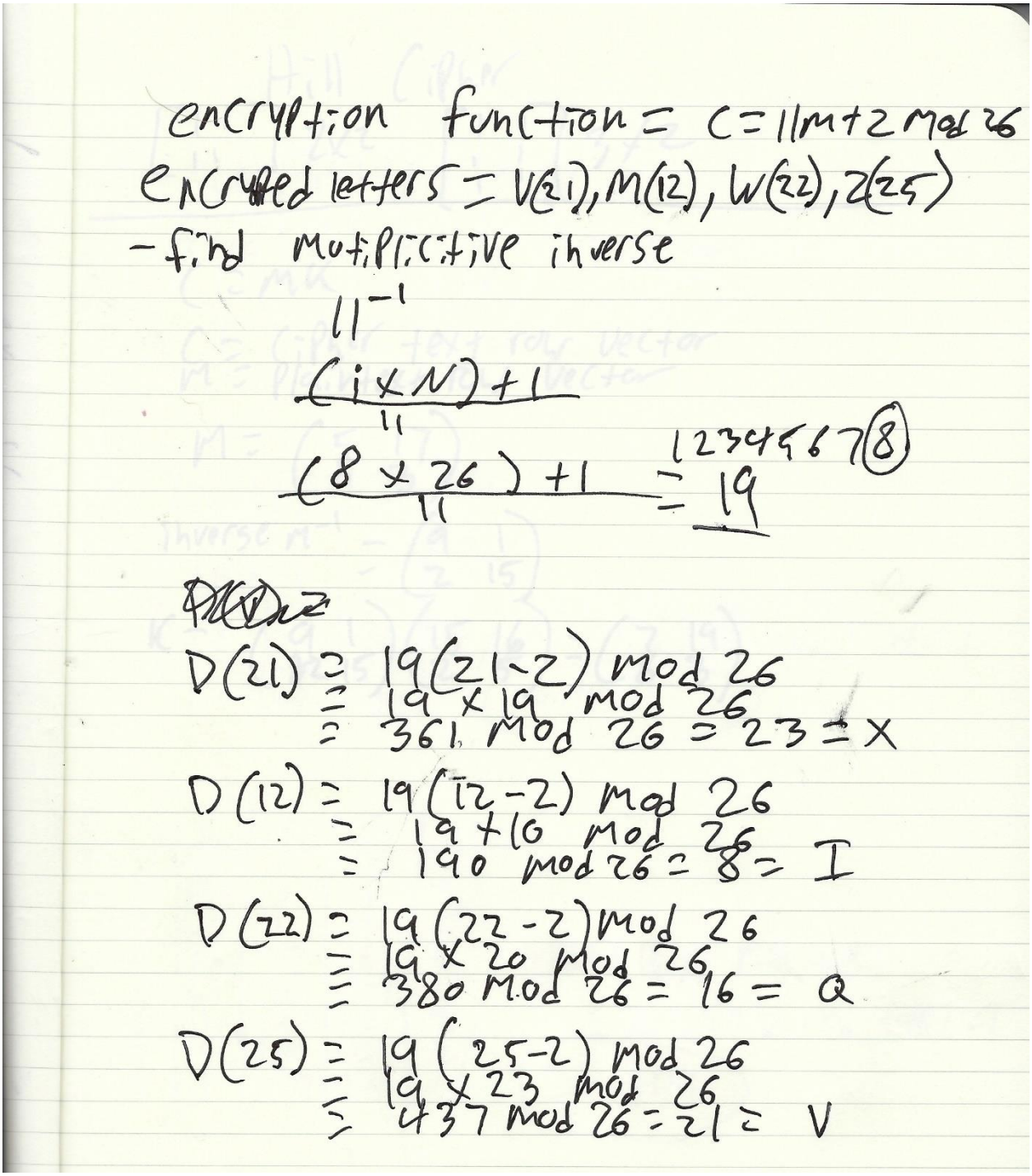
$$C_m = 5M + 7 \bmod 26$$

~~$C_e = 3 \times 7 + 7 \bmod 26$~~

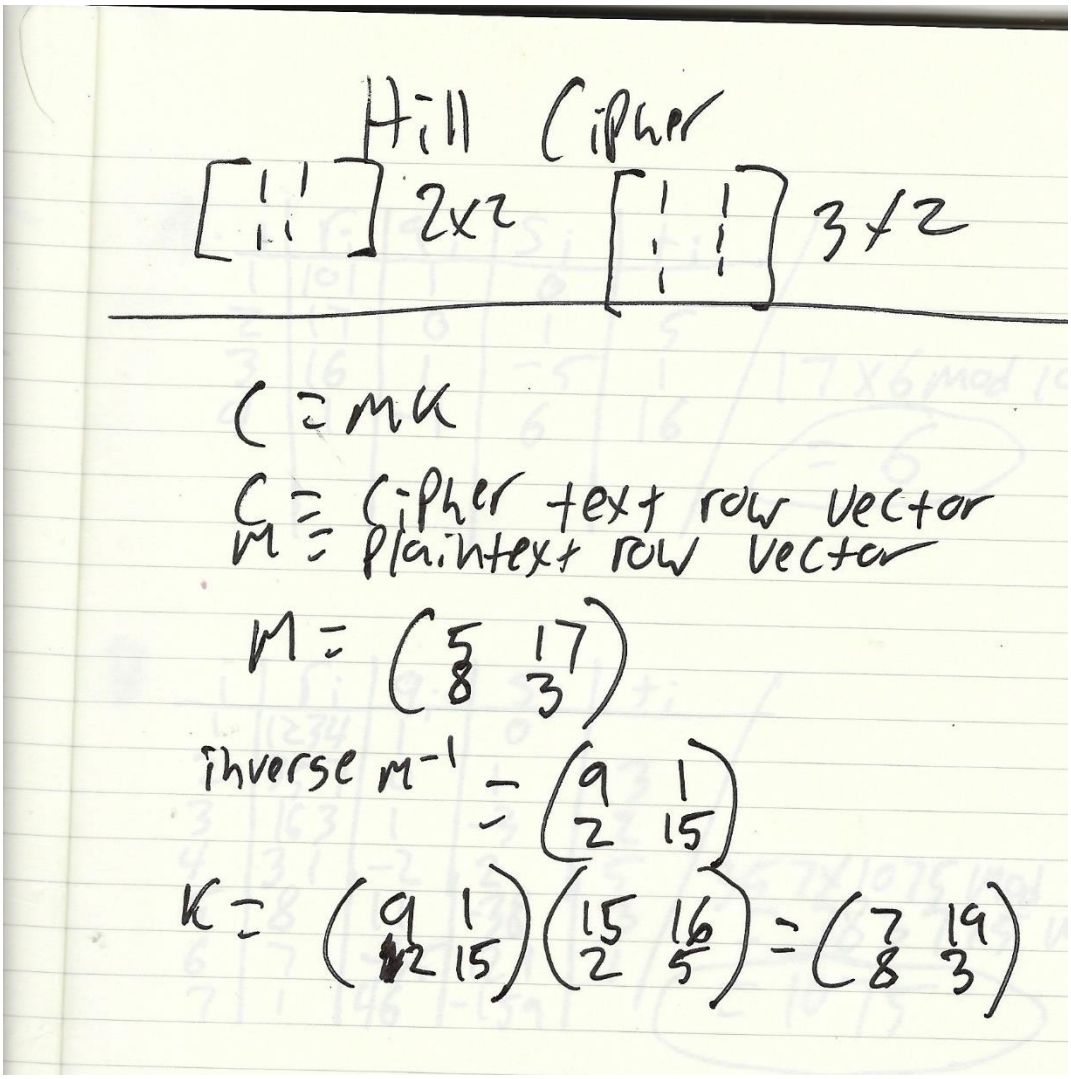
$C_n = 5 \times 7 + 7 \bmod 26 = 42 \bmod 26 = 16 = Q$
$C_e = 5 \times 4 + 7 \bmod 26 = 27 \bmod 26 = 1 = B$
$C_i = 5 \times 11 + 7 \bmod 26 = 62 \bmod 26 = 10 = K$
$C_p = 5 \times 15 + 7 \bmod 26 = 82 \bmod 26 = 4 = E$
$C_m = 5 \times 12 + 7 \bmod 26 = 67 \bmod 26 = 15 = P$
$C_e = 5 \times 4 + 7 \bmod 26 =$

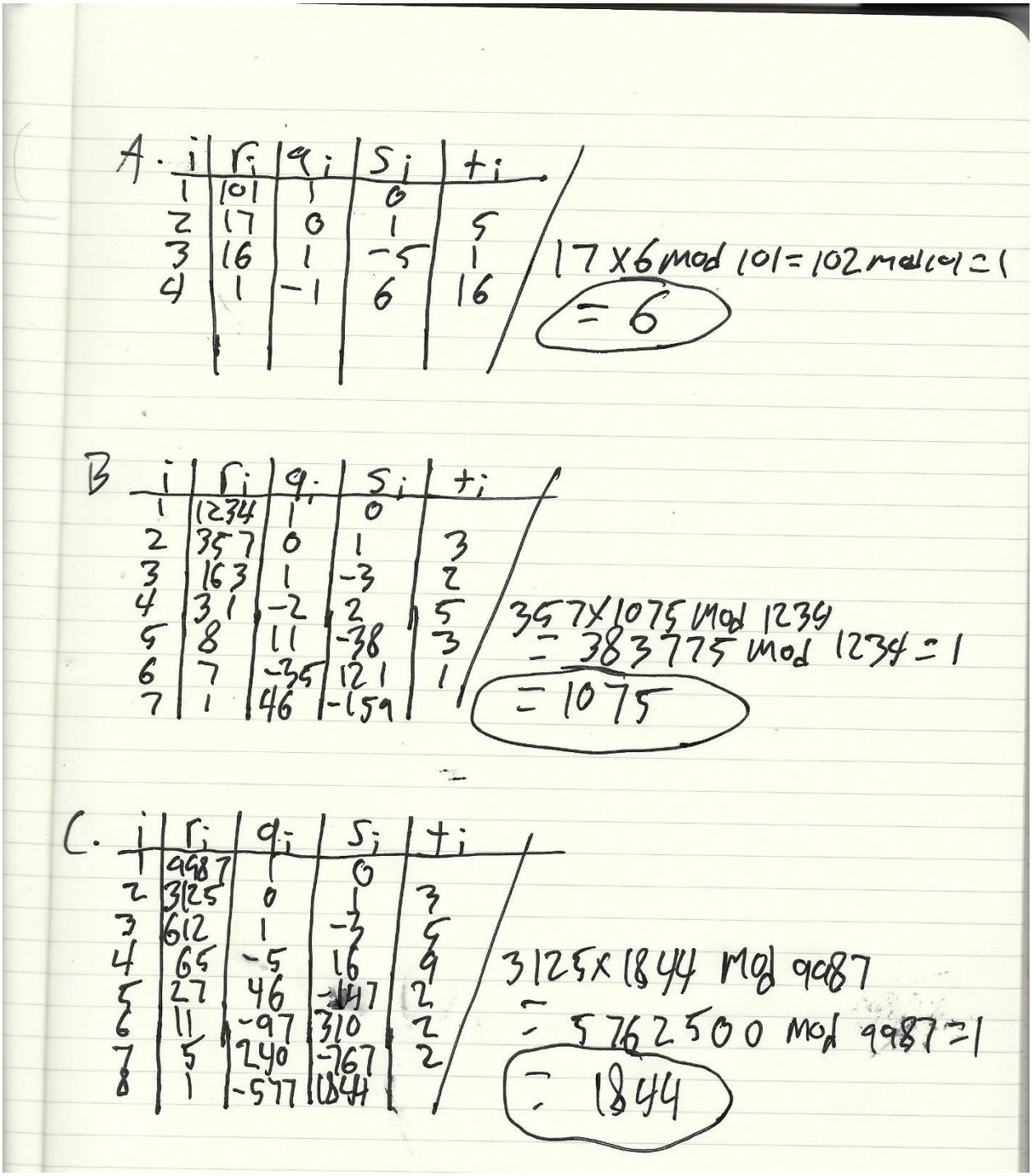
QBKEPB

2.


encryption function = C = 11m + 2 mod 26
encrypted letters = V(21), M(12), W(22), Z(25)
- find multiplicative inverse
11^-1
(i x N) + 1
11
(8 x 26) + 1 = 19
11
1 2 3 4 5 6 7 (8)
D(21) = 19(21-2) mod 26
= 19 x 19 mod 26
= 361 mod 26 = 23 = X
D(12) = 19(12-2) mod 26
= 19 + 10 mod 26
= 190 mod 26 = 8 = I
D(22) = 19(22-2) mod 26
= 19 x 20 mod 26
= 380 mod 26 = 16 = Q
D(25) = 19(25-2) mod 26
= 19 x 23 mod 26
= 437 mod 26 = 21 = V

3.


Hill Cipher
[! ! ; ! !] 2x2
[! ! ; ! !] 3x2
C = mK
C = Cipher text row vector
M = Plaintext row vector
M = (5 17 ; 8 3)
inverse m^-1 = (9 1 ; 2 15)
K = (9 1 ; 2 15)(15 16 ; 2 5) = (7 19 ; 8 3)



A.

i	r_i	q_i	s_i	t_i
1	101	1	0	
2	17	0	1	5
3	16	1	-5	1
4	1	-1	6	16

$17 \times 6 \bmod 101 = 102 \bmod 101 = 1$

$= 6$

B

i	r_i	q_i	s_i	t_i
1	1234	1	0	
2	357	0	1	3
3	163	1	-3	2
4	31	-2	7	5
5	8	11	-38	3
6	7	-35	121	1
7	1	46	-159	

$357 \times 1075 \bmod 1234$

$= 383775 \bmod 1234 = 1$

$= 1075$

C.

i	r_i	q_i	s_i	t_i
1	9987		0	
2	3125	0	1	3
3	612	1	-3	5
4	65	-5	16	9
5	27	46	-147	2
6	11	-97	310	2
7	5	240	-767	2
8	1	-577	1844	

$3125 \times 1844 \bmod 9987$

$= 5762500 \bmod 9987 = 1$

$= 1844$

4.
5.

python3

```
def brute(cipher):
    length=len(cipher)
    for key in range(1,26):
        plaintext=""
        for i in range(length):
            reorder=(ord(cipher[i])-ord('A')-key)%26
            if(reorder<0):
                reorder=reorder+26
            reorder=reorder+ord('A')
            plaintext=plaintext+chr(reorder)
        print("key#",key,"plaintext=",plaintext)
brute('BEEAKFYDJXUQYHYJIQRYHTYJIQFBQDUYJIIKFUHCQD')
```

key# 1 plaintext= ADDZJEXCIWTPXGXIHPQXGSXIHPEAPCTXIHHJETGBPC

key# 2 plaintext= ZCCYIDWBHVSOWFWHGOPWFRWHGODZOBSWHGGIDSFAOB

key# 3 plaintext= YBBXHCVAGURNVEVGFNOVEQVGFNCYNARVGFFHCREZNA

key# 4 plaintext= XAAWGBUZFTQMUDUFEMNUDPUFEMBXMZQUFEEGBQDYMZ

key# 5 plaintext= WZZVFATYESPLTCTEDLMTCOTEDLAWLYPTEDDFAPCXLY

key# 6 plaintext= VYYUEZSXDROKSBSDCKLSBNSDCKZVKXOSDCCEZOBWKX

key# 7 plaintext= UXXTDYRWCQNJRARCBJKRAMRCBJYUJWNRCBBDYNAVJW

key# 8 plaintext= TWWSCXQVBPMIQZQBAIJQZLQBAIXTIVMQBAACXMZUIV

key# 9 plaintext= SVVRBWPUAOLHPYPAZHIPYKPAZHWSHULPAZZBWLYTHU

key# 10 plaintext= RUUQAVOTZNKGOXOZYGHOXJOZYGVRGTKOZYYAVKXSGT

key# 11 plaintext= QTTPZUNSYMJFNWNYXFGNWINYXFUQFSJNYXXZUJWRFS

key# 12 plaintext= PSSOYTMRXLIEMVMXWEFMVHMXWETPERIMXWWYTIVQER

key# 13 plaintext= ORRNXSLQWKHDLULWVDELUGLWVDSODQHLWVVXSHUPDQ

key# 14 plaintext= NQQMWRKPVJGCKTKVUCDKTFKVUCRNCPGKVUUWRGTOCP

key# 15 plaintext= MPPLVQJOUIFBJSJUTBCJSEJUTBQMBOFJUTTVQFSNBO

key# 16 plaintext= LOOKUPINTHEAIRITSABIRDITSAPLANEITSSUPERMAN

key# 17 plaintext= KNNJTOHMSGDZHQHSRZAHQCHSRZOKZMDHSRRTODQLZM

key# 18 plaintext= JMMISNGLRFCYGPGRQYZGPBGRQYNJYLCGRQQSNCPKYL

key# 19 plaintext= ILLHRMFKQEBXFOFQPXYFOAFQPXMIXKBFQPPRMBOJXK

key# 20 plaintext= HKKGQLEJPDAWENEPOWXENZEPOWLHWJAEPOOQLANIWJ

key# 21 plaintext= GJJFPKDIOCZVDMDONVWDMYDONVKGVIZDONNPKZMHVI

key# 22 plaintext= FIIEOJCHNBYUCLCNMUVCLXCNMUJFUHYCNMMOJYLGUH

key# 23 plaintext= EHHDNIBGMAXTBKBMLTUBKWBMLTIETGXBMLLNIXKFTG

key# 24 plaintext= DGGCMHAFLZWSAJALKSTAJVALKSHDSFWALKKMHWJESF

key# 25 plaintext= CFFBLGZEKYVRZIZKJRSZIUZKJRGCREVZKJJLGVIDRE