Unicity distance of Vernam with key lengths

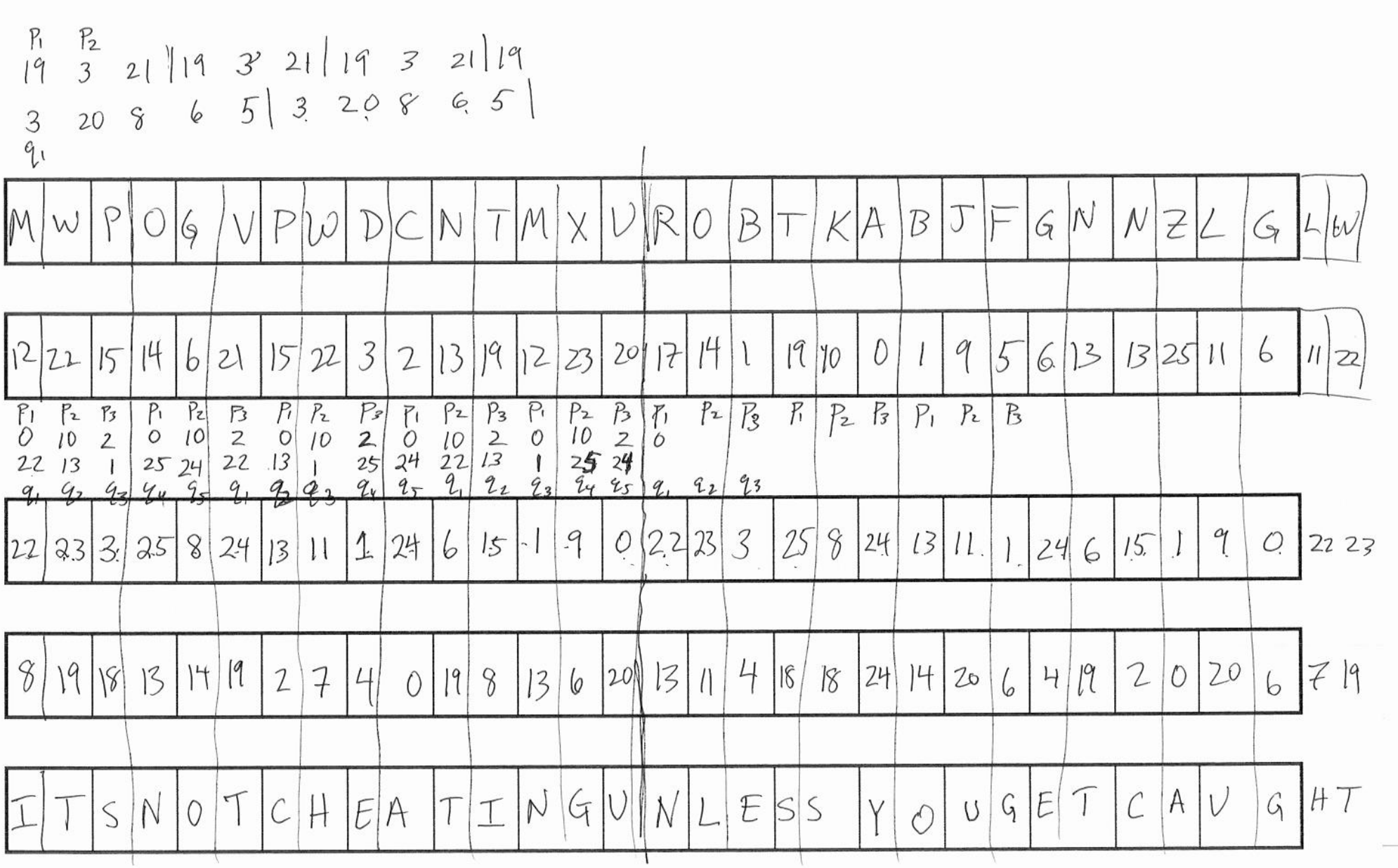
p & q $\gcd(p,q) = 1$

$H(K) = \log_2(26^{P+q-1})$ $H(M) = F \cdot N$ $H(C) = \log_2(26^N)$

(4) The following cyphertext was encrypted with the Vernam system with two keys of length 3 and 5 respectively.

MWPOG VPWDC NTMXU ROBTK ABJFG NNZLG LW

The cyphertext DCN starting at position 9 is known to be 'eat' and the letters OBTK at position 17 correspond to the word 'less.' Recover the message.



A	0		F	5		K	10		P	15		U	20		Z	25														
B	1		G	6		L	11		Q	16		V	21																	
C	2		H	7		M	12		R	17		W	22																	
D	3		I	8		N	13		S	18		X	23																	
E	4		J	9		O	14		T	19		Y	24																	

Vernam

gcd

given r & s

find k & ℓ s.t. $k \cdot r + \ell \cdot s = \gcd(r,s)$

solve linear equations of the form $ax \equiv b \pmod{n}$

$a^b \pmod{n}$ - calculate

$a^{\phi(n)} \equiv 1 \pmod{n}$ Euler-Fermat Theorem.

Encrypt & decrypt RSA

Legendre symbol

Jacobi symbol - fast formula for computing

Hint: Jacobi symbol $J(a,p) = \left(\frac{a}{p}\right)$ if p is prime.

Test if a number is prime or not.

$$\left(\frac{26}{53}\right) = J(26,53)$$

$$= J(53 \pmod{26}, 26)(-1)^{(26-1)(53-1)/8}$$

$$= J(1,26)(-1)^{25 \cdot 52/4} \quad ?$$

$$= J(1,26)(-1) = -1$$

$$J(a,n) = J(n \bmod a, a)(-1)^{(a^2-1)(n^2-1)/8} \quad ?$$

$$J(1,n) = 1$$

$$J(2a,n)$$

$$= J(26/2, 53)(-1)^{53^2-1/8}$$

$$= J(13,53)(-1)$$

$$= -J(53 \bmod 13, 13)(-1)^{(13-1)(53-1)/4}$$

$$= -J(1,13)$$

$$= -1$$

$\therefore$ no solution

$\frac{52 \cdot 54}{4} \quad \frac{}{2} = -$

26
676

$$13 \overline{)53}$$
$$52$$
$$4 \text{ r } 1$$

$28^2 \equiv 14 \pmod{77}$

$28^4 \equiv 14^2 \equiv 42$

$28^7 \equiv 28^4 \cdot 28^2 \cdot 28^1$

$\equiv 42 \cdot 14 \cdot 28$

$\equiv 63$ 7

$28 \cdot 28 = 784$

$14 \cdot 14 = 196$

$42 \cdot 7 = 294$

$196 = 77 \cdot 2 + 42$

$294 = 77 \cdot 3 + 63$

S	U	N
↓	↓	↓
18	20	13

$18 \cdot 26^0 + 20 \cdot 26^1 + 13 \cdot 26^2$

Any number can be written base 26 into

$n = a_0 \cdot 26^0 + a_1 26^1 + a_2 26^2 + \cdots + a_k 26^k$

where $0 \le a_i \le 25$

Instructions of problem say encrypt S, then U, then N

$m = 77 \quad \phi(m) = 60 = (7-1)(11-1)$

to encrypt "S" with RSA $e = 7$

$28^7 \pmod{77} \equiv 63$

$30^7 \pmod{77} \equiv$ } do at home

$23^7 \pmod{77} \equiv$ }

---

the decrypting exponent is the value d s.t.

$d \cdot e \equiv d \cdot 7 \equiv 1 \pmod{60}$

$60 = 8 \cdot 7 + 4 \quad = 2(60 - 8 \cdot 7) - 7 = 2 \cdot 60 - 17 \cdot 7$

$7 = 1 \cdot 4 + 3 \quad = 4 - (7 - 4) = 2 \cdot 4 - 7$

$4 = 1 \cdot 3 + 1 \quad 1 = 4 - 3 \quad 1 = -17 \cdot 7 + 2 \cdot 60$

$d \equiv (-17) \equiv 43 \pmod{60} \quad 1 \equiv (-17) \cdot 7 \pmod{60}$

$m = 77 \quad e = 7 \quad d \equiv 43$

$73^{43} \pmod{77}$

$\equiv (-4)^{43} \pmod{77}$

$\equiv (-1)^{43} \cdot (2^2)^{43} \pmod{77}$

$\equiv -2^{86} \pmod{77}$

$\equiv -2^{26} \cdot 2^{60} \pmod{77}$

$\equiv -2^{16} \cdot 2^8 \cdot 2^2$

$\equiv -5^4 \cdot 5^2 \cdot 4$

$\equiv -5^6 \cdot 4$

$\equiv -9 \cdot 5^2 \cdot 4$

$\equiv -9 \cdot 25 \cdot 4$

$\equiv -900$

$\equiv -53$

$\equiv 24$

$5^2 \equiv 25$

$2^{60} \equiv 1 \pmod{77}$

$2^2 \equiv 4$

$2^4 \equiv 4^2 \equiv 16$

$2^8 \equiv 16^2 \equiv 256$

$\equiv 25 \equiv 5^2$

$2^{16} \equiv (2^8)^2 \equiv (5^2)^2 \equiv 5^4$

$25 \times 25 = 625$

$625 \div 77 = 8$ remainder 9

$256 \div 77 = 3$ remainder 25

$900 \div 77 = 11$ remainder 53

4. (a) Compute $J(13, 4819)$, the Jacobi symbol of 13 and 4819.

   (b) Compute $13^{2409} \bmod 4819$. (Hint: $13^{39} = 1 \bmod 4819$)

   (c) Is 4819 prime? Why or why not.

3. (a) Compute $(\frac{13}{29})$, the Legendre symbol of 13 and 29.

   (b) Is there a value x such that $x^2 = 13 \bmod 29$? Explain.

(4) Factor 69689 given that $277^2 \equiv 17529^2 \equiv 7040 \pmod{69689}$.

(5) Determine if $(x+6)^2 \equiv x^2 + 12x + 36 \equiv 36 - 10 \equiv 26 \pmod{53}$

$$x^2 + 12x + 10 \equiv 0 \pmod{53}$$

has a solution. Hint: complete the square.

(2) Alice and Bob decided to communicate using a key arrived at from the Diffie-Hellman key exchange system. They first agree on a modulus of 53 and a primitive root of 22. Alice sends to Bob her public key of 19 and Bob sends to Alice his public key of 37. You intercept these exchanges. Use the table of powers of 2 below to help recover their secret keys S_A and S_B and their common key $22^{S_A S_B} (mod\ 53)$.

(3) Using the same primitive root and modulus, Alice sends Bob the message $(Y, Z) = (19, 39)$ using the ElGamal system. What was the message sent to Bob?

has a solution iff $(\frac{26}{53}) = 1$

k	1	2	3	4	5	6	7	8	9	10	11	12	13
$2^k (mod\ 53)$	2	4	8	16	32	11	22	44	35	17	34	15	30

k	14	15	16	17	18	19	20	21	22	23	24	25	26
$2^k (mod\ 53)$	7	14	28	3	6	12	24	48	43	33	13	26	52

k	27	28	29	30	31	32	33	34	35	36	37	38	39
$2^k (mod\ 53)$	51	49	45	37	21	42	31	9	18	36	19	38	23

k	40	41	42	43	44	45	46	47	48	49	50	51	52
$2^k (mod\ 53)$	46	39	25	50	47	41	29	5	10	20	40	27	1

$x^2 \equiv a \pmod{p}$ has a solution if $(\frac{a}{p}) = 1$