Problem Sheet 5
Solutions

Exercise (1). See the solution in tutorials.

Exercise (2).

(a) First, multiplying each ciphertext message unit by 23 mod 61 we obtain that

14, 25, 89, 3, 65, 24, 3, 49, 89, 24, 41, 25, 68, 41, 71 →

17, 26, 34, 8, 31, 3, 8, 29, 34, 3, 28, 26, 39, 28, 47.

Similarly, multiplying each number of the public key 57,14,3,24,8 by 23 mod 61 we obtain 30, 17, 8, 3, 1. Hence, we have a superincreasing sequence

$$1, 3, 8, 17, 30.$$

Applying superincreasing knapsack problem algorithm we have the following.

$17 \to 0 \cdot 30 + 1 \cdot 17 + 0 \cdot 8 + 0 \cdot 3 + 0 \cdot 1 \to (01000)_2 = 2^3 \to$ I.

$26 \to 17 + 8 + 1 \to (01101)_2 \to 2^3 + 2^2 + 1 = 13 \to$ N.

$34 \to 30 + 3 + 1 \to (10011)_2 \to 2^4 + 2 + 1 = 12 \to$ T.

$8 \to 8 \to (01100)_2 \to 4 \to$ E.

$31 \to 30 + 1 \to (10001)_2 \to 2^4 + 1 = 17 \to$ R.

$3 \to 3 \to (00010)_2 \to 2 \to$ C.

$29 \to 17 + 8 + 3 + 1 \to (01111)_2 \to 2^3 + 2^2 + 2 + 1 = 15 \to$ P.

$28 \to 17 + 8 + 3 \to (01110)_2 \to 2^3 + 2^2 + 2 = 14 \to$ O.

$39 \to 30 + 8 + 1 \to (10101)_2 \to 2^4 + 2^2 + 1 = 12 \to$ V.

$47 \to 30 + 17 \to (11000)_2 \to 2^4 + 2^3 = 24 \to$ Y.

`Answer`. INTERCEPTCONVOY.

(b) TENFOUR → 19 4 13 5 14 20 17. Representing these values as numbers to the base 2, and then applying the encryption key 57,14,3,24,8 we obtain the following.

T → $19 = 2^4 + 2 + 1 = (10011)_2 = 57 + 24 + 8 = 89$;

E → $4 = 2^2 = (00100)_2 = 3$;

N → $13 = 2^3 + 2^2 + 1 = (01101)_2 = 14 + 3 + 8 = 25$;

F → $5 = 2^2 + 1 = (00101)_2 = 3 + 8 = 11$;

O → $14 = 2^3 + 2^2 + 2 = (01110)_2 = 14 + 3 + 24 = 41$;

U → $20 = 2^4 + 2^2 = (10100)_2 = 57 + 3 = 60$;

R → $17 = 2^4 + 1 = (10001)_2 = 57 + 8 = 65$.

`Answer.` 89,3,25,11,41,60,65.

Exercise (3)
The numbering of alphabet symbols is

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

U	V	W	X	Y	Z	⊔	?	!	.	’	$
20	21	22	23	24	25	26	27	28	29	30	31

We are given the encryption sequence $\{w_i\}$, and the secret key $b = 30966$ and modulus $m = 47107$. The superincreasing sequence is $\{v_i\}$ where $v_i \equiv bw_i$ mod m. We then readily calculate the terms of the superincreasing sequence, as in the following table (the second row is simply a numbering of the terms of the sequence):

1	2	5	9	20	39	80	163	330	691	1351	2710	5611	11376	23001
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

Note that the superincreasing sequence is actually in reverse order to the order of the given public key sequence.

Now we decrypt the ciphertext, unit by unit.

1. 152472. Multiplying by b and reducing mod m, we get $152472 \cdot 30966 \mod 47107 = 7556$. Solving the superincreasing knapsack problem for 7556:

$$7566 = 5611 + 1351 + 330 + 163 + 80 + 20 + 1$$

which has decimal equivalent (using the numbering in the previous table)

$$2^{12} + 2^{10} + 2^8 + 2^7 + 2^6 + 2^4 + 2^0 = 5585.$$

Since we are using units of length 3, 5585 is the decimal equivalent of the unit in base 32 (= size of the alphabet). That is,

$$5585 = 5 \cdot 32^2 + 14 \cdot 32 + 17$$

so the first unit of plaintext is $5, 14, 17$ i.e. FOR in the alphabet symbols.

2. 116116. $116116 \cdot 30966 \mod 47107 = 17853$. Then

$$17853 = 11376 + 5611 + 691 + 163 + 9 + 2 + 1$$

which has decimal equivalent

$$2^{13} + 2^{12} + 2^9 + 2^7 + 2^3 + 2^1 + 2^0 = 12939.$$

Now

$$12939 = 12 \cdot 32^2 + 20 \cdot 32 + 11$$

so the second unit of plaintext is $12, 20, 11$ i.e. MUL

3. 68546. $68546 \cdot 30966 \mod 47107 = 1123$. Then

$$1123 = 691 + 330 + 80 + 20 + 2$$

which has decimal equivalent

$$2^9 + 2^8 + 2^6 + 2^4 + 2^1 = 850.$$

Now

$$852 = 0 \cdot 32^2 + 26 \cdot 32 + 18$$

so the third unit of plaintext is $0, 26, 29$ i.e. $A \sqcup S165420$. $165420 \cdot 30966 \mod 47107 = 27647$. Then

$$27647 = 23001 + 2710 + 1351 + 330 + 163 + 80 + 9 + 2 + 1$$

which has decimal equivalent

$$2^{14} + 2^{11} + 2^{10} + 2^8 + 2^7 + 2^6 + 2^3 + 2^1 + 2^0 = 19915.$$

Now

$$19915 = 19 \cdot 32^2 + 14 \cdot 32 + 11$$

so the fourth unit of plaintext is $19, 14, 11$ i.e. TOL

4. 168261. $168261 \cdot 30966 \bmod 47107 = 6177$. Then

$$6177 = 5611 + 330 + 163 + 39 + 20 + 9 + 5$$

which has decimal equivalent

$$2^{12} + 2^8 + 2^7 + 2^5 + 2^4 + 2^3 + 2^2 = 4540.$$

Now

$$4540 = 4 \cdot 32^2 + 13 \cdot 32 + 28$$

so the fifth unit of plaintext is $4, 13, 28$ i.e. EN!

Assembling the results of (1)−(5) above we get the plaintext FORMULA␣STOLEN!
`Answer.` FORMULA STOLEN!

Exercise (4).

(a) First, using the formula $w_i = v_i \cdot a$ mod m we obtain the encryption key: 7, 21, 35, 29, 24. Next, ALGEBRA $\rightarrow$ 0, 11, 6, 4, 1, 17, 0. Now re-writing the key in reverse order, i.e. as 24, 29, 35, 21, 7, we have the following.

A $\rightarrow 0 = 0{\cdot}2^4{+}0{\cdot}2^3{+}0{\cdot}2^2{+}0{\cdot}2^1{+}0{\cdot}2^0 = (00000)_2 = 0{+}0{+}0{+}0{+}0 = 0$;

L $\rightarrow 11 = 2^3 + 2 + 1 \rightarrow (01011)_2 \rightarrow 29 + 21 + 7 = 57$

G $\rightarrow 6 = 2^2 + 2 \rightarrow (00110)_2 \rightarrow 35 + 21 = 56$

E $\rightarrow 4 = 2^2 \rightarrow (00100)_2 \rightarrow 35$

B $\rightarrow 1 = \rightarrow (00001)_2 \rightarrow 7$

R $\rightarrow 17 = 2^4 + 1 \rightarrow (10001)_2 \rightarrow 24 + 7 = 31$

`Answer` 0, 57, 56, 35, 7, 31, 0.

(b) First we have that the decryption key b $= a^{-1}$mod m $= 7^{-1}$mod 41 $=$ 6 (because $7 \cdot 6 = 42$. Next multiplying each number in the cryptotext by 6 mod 41 we obtain 4, 0, 31. Now applying knapsack algorithm for the sequence 1, 3, 5, 10, 21 we obtain the following.

$4 = 0 \cdot 21 + 0 \cdot 10 + 0 \cdot 5 + 1 \cdot 3 + 1 \cdot 1 \rightarrow (00011)_2 = 2 + 1 = 3 \rightarrow D$

$0 \rightarrow 0 \rightarrow A$

$31 \rightarrow 21 + 10 \rightarrow (11000)_2 \rightarrow 2^4 + 2^3 = 24 \rightarrow Y$.

`Answer.` DAY.