1. (a) (i) [**2 marks**] Find an inverse of 5 modulo 37.

(ii) [**2 marks**] Solve the congruence $5x \equiv 4 \pmod{37}$.

(b) (i) [**2 marks**] Find the order of 3 modulo 11.

(ii) [**2 marks**] Compute the residue of 3^{2016} modulo 11.

(c) [**2 marks**] Complete the definition: a function $f(n)$ of a positive integer variable n is said to be *multiplicative* if ....

(d) [**2 marks**] Find a quadratic polynomial $Q(x) = ax^2 + bx + c$, where the coefficients a, b, c belong to $\{0, 1, 2, 3, 4, 5, 6\}$, such that the following all hold:

$$\begin{aligned} Q(1) &\equiv 2 \pmod{7}, \\ Q(2) &\equiv 4 \pmod{7}, \\ Q(3) &\equiv 1 \pmod{7}. \end{aligned}$$

2. (a) [**3 marks**] A Vigenère cipher with encryption key `FOX` has been used to produce the ciphertext `ROQMG`. What was the plaintext?

(b) [**3 marks**] Suppose you are given a long ciphertext in capital letters (of the ordinary alphabet) and told that it was produced by enciphering ordinary English text using either a simple substitution cipher or a transposition cipher. What statistical feature of the ciphertext would you consider to decide which of the two types of cipher was used, and why?

(c) [**3 marks**] Suppose that an RSA cryptosystem has public key $(119, 5)$. What is the decryption exponent?

(d) [**3 marks**] Suppose that you are an Elgamal user with public key $(59, 2, 5)$ and private key 6. Note that this is consistent, because $2^6 \equiv 5 \pmod{59}$. You receive the message $\langle 3, [21, 4] \rangle$. Decrypt it.

Tutorials in week 13 - practise past exam questions from 2011, 2012.

Questions from 2016 Exam.

Q1 (a) (i) Find $5^{-1} \pmod{37}$.

We try: 1, 38, 75. The last one is divisible by 5 $\Rightarrow$ $5 \cdot 15 = 75 \equiv 1 \pmod{37}$

$\Rightarrow 5^{-1} \equiv 15 \pmod{37}$.

Another way: EEA:

$37 = 7 \cdot 5 + 2$

$5 = 2 \cdot 2 + 1$

$\Rightarrow 1 = 5 - 2 \cdot 2 = 5 - 2(37 - 7 \cdot 5) = 15 \cdot 5 - 2 \cdot 37$

$\Rightarrow 15 \equiv 5^{-1} \pmod{37}$.

Q1 (a) (ii)

$5x \equiv 4 \pmod{37}$

$\Leftrightarrow x \equiv 5^{-1} \cdot 4 \pmod{37}$

$x \equiv 15 \cdot 4 \equiv 23 \pmod{37}$.

Q1 (b) (i) $\mathrm{Ord}_{11}(3) = ?$

n	1	2	3	4	5	6
$3^n \pmod{11}$	3	9	5	4	1	

$\Rightarrow \mathrm{ord}_{11}(3) = 5$.

We can use the fact : $\text{ord}_m(a) \mid \varphi(m)$.

Q 1(b)(ii) $3^{2016} \pmod{11}$

$$3^{2016} = 3^{403\cdot 5+1} \equiv 3^1 \equiv 3 \pmod{11}.$$

Q 1(d) $Q(x) = ax^2+bx+c$ — ?

$$\begin{cases} Q(1) \equiv 2 \pmod 7 \\ Q(2) \equiv 4 \pmod 7 \\ Q(3) \equiv 1 \pmod 7 \end{cases}$$

We use Lagrange interpolation formula:

$$Q(x) = 2\cdot\frac{(x-2)(x-3)}{(1-2)(1-3)} + 4\cdot\frac{(x-1)(x-3)}{(2-1)(2-3)} + 1\cdot\frac{(x-1)(x-2)}{(3-1)(3-2)}$$

$$\equiv (x-2)(x-3) - 4(x-1)(x-3) + 2^{-1}(x-1)(x-2)$$

$$\equiv (x^2-5x+6) - 4(x^2-4x+3) + 4(x^2-3x+2)$$

$$\equiv \cancel{7}\, x^2 + 6x + 2 \pmod 7.$$

Q 2(a) Vigenère cipher with key FOX has been used to produce ROQMG

Plaintext — ?

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

$$\begin{array}{ccccc} R & O & Q & M & G \\ 17 & 14 & 16 & 12 & 6 \\ F & O & X & F & O \\ 5 & 14 & 23 & 5 & 14 \\ \hline 12 & 0 & 19 & 7 & 18 \\ M & A & T & H & S \end{array}$$

Q2(b) You are given long ciphertext from the ordinary English text. Enciphered by either simple substitution or by transposition cipher. Which one?

We consider frequency of single letters. If the distribution of frequencies is close to that of standard English text then most probably a transposition cipher was used(it does not change the distribution). Otherwise, most probably simple substitution cipher was used (it changes the distribution).

Q2(c) RSA cryptosystem with key (119, 5) Decryption exponent - ?

$$\underset{\underset{n}{\uparrow}}{119}, \quad \underset{\underset{e}{\uparrow}}{5}$$

Decryption exponent satisfies $d \cdot e \equiv 1 (\mathrm{mod}\ \varphi(n))$

Factoring $119 = 7 \cdot 17$

$\varphi(119) = 6 \cdot 16 = 96$

$d \equiv 5^{-1} \pmod{96} \equiv -19 \equiv 77 \pmod{96}$

(because $5 \cdot 19 \equiv 95 \equiv -1 \pmod{96}$).