Data provided: Data Sheet

MAS345

The University Of Sheffield.

SCHOOL OF MATHEMATICS AND STATISTICS **Spring Semester 2014–2015**

Codes and Cryptography **2 hours 30 minutes**

Attempt all the questions. The allocation of marks is shown in brackets.

1 (i) Write down a parity check matrix for, and the dimension of, the 10-bit International Book Standard Number ISBN-10 over the field $\mathbb{F}_{11}$. ***(2 marks)***

(a) Let $x, y \in \mathbb{F}_{11}$. Show that $xyxyxyxyxy$ is an ISBN-10 codeword if and only if $x = y$. ***(4 marks)***

(b) Let $v, w, x, y \in \mathbb{F}_{11}$. Show that there exists a unique $z \in \mathbb{F}_{11}$ such that $vwxyzvwxyz$ is an ISBN-10 codeword. ***(3 marks)***

(c) Let $v, w, x, y, z \in \mathbb{F}_{11}$. Show that if $vwxyzvwxyz$ is an ISBN-10 codeword and $w \neq z$ then $vzxywvzxyw$ is not an ISBN-10 codeword. ***(3 marks)***

(ii) Let C be the linear code of length 7 over the field $\mathbb{F}_2$ with generator matrix

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

(a) Find a parity check matrix for C and write down a parity check matrix for the dual code $C^{\perp}$. ***(6 marks)***

(b) How many distinct codewords are there in C and how many distinct codewords are there in $C^{\perp}$? ***(2 marks)***

(c) Find codewords $c \in C$ and $v \in C^{\perp}$ such that $c + v = (1\ 0\ 0\ 0\ 0\ 0\ 1)$. ***(5 marks)***

2 (i) Let C be an $[n, k, 3]$-linear code over $\mathbb{F}_p$ and let H be a parity check matrix for C with columns $h_1, h_2, \ldots, h_n$. Let $a = a_1 a_2 \ldots a_i \ldots a_n \in C$ and let $b = a_1 a_2 \ldots b_i \ldots a_n$ be obtained from a by a single error which occurs in the ith bit. Show that $Hb^T = (b_i - a_i)h_i$. ***(3 marks)***

(ii) Let F be an alphabet with q elements and let $n \geq 2$ be an integer. Let r be an integer with $0 \leq r \leq n$ and let $c \in F^n$. Show that the number of elements in the Hamming sphere $S(c, r)$ of radius r centred at c is

$$\sum_{j=0}^{r} (q-1)^j \binom{n}{j}.$$

(4 marks)

(iii) Write down, without proof, the *Sphere-Packing Bound* for an (n, M, d)-code C over an alphabet F with q elements and explain what it means to say that C is perfect. ***(3 marks)***

(iv) Let H be the matrix

$$\begin{pmatrix} 1 & 0 & 1 & 2 & 3 & 4 \\ 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

over the field $\mathbb{F}_5$. Let C be the linear code over $\mathbb{F}_5$ with parity check matrix H.

(a) Show that H is a perfect code, giving reasons for your values for the dimension k and the minimum distance d of C. ***(6 marks)***

(b) A company produces postcards of wild life and assigns a codeword from C to each of their postcards. A customer Asterix tries to order the crocodile card but mistypes one digit of the codeword and submits the word 321040. Use (i) to find the codeword of the crocodile card. ***(3 marks)***

(c) Let D be a perfect $[n, k, 3]$-linear code over $\mathbb{F}_p$ for some prime p, some length n and some dimension k. Let a be a codeword in D such that the final digits a_{n-1} and a_n are distinct. Let b be obtained from a by transposing these two digits. Explain why $b \notin D$ and why there is a unique codeword $v \in D$ such that $d(b, v) = 1$. ***(3 marks)***

When the company in (b) receives an order with an invalid codeword they assume that a single error has been made. A second customer Boadicea tries to order the crocodile card but transposes the last two digits of the correct codeword. She receives a postcard with a picture of a wildebeest. Find the codeword of the wildebeest card. ***(3 marks)***

3 (i) A message is written in capital letters and is encrypted using first Caesar encryption with key M and then the one-time pad method with key *RED SAILS IN THE SUNSET*, both modulo 26 with the correspondence shown on the Data Sheet. The encrypted message is

WYBIFIDS.

Decrypt the message. ***(4 marks)***

(ii) Messages are broken up into units that can be encoded using the 121 elements of $\mathbb{F}_{11}^2$, with 10 written as X. Elements of $\mathbb{F}_{11}^2$ are then written as columns and encrypted using 2-dimensional affine encryption modulo 11, with the transformation $f : \mathbb{F}_{11}^2 \to \mathbb{F}_{11}^2$ given by $f(V) = KV + L$, where

$$K = \begin{pmatrix} 3 & 5 \\ 7 & 9 \end{pmatrix} \text{ and } L = \begin{pmatrix} 6 \\ 7 \end{pmatrix}.$$

Find $V \in \mathbb{F}_{11}^2$ such that V is encrypted as $(3\ X)^T$ and find $W \in \mathbb{F}_{11}^2$ such that W is encrypted as itself. ***(6 marks)***

(iii) Throughout this part, you may use the squares in $\mathbb{F}_{97}$ shown on the data sheet. A society uses the key-exchange system of Diffie-Hellman to produce shared keys that are non-zero elements of $\mathbb{F}_p$ for a chosen prime p. The society changes the prime p and generator of $\mathbb{F}_p$ that they use each month.

(a) In May, they choose $p = 97$ with the generator $g = 17$. Write down the maximal proper divisors of 96 and show that 17 is indeed a generator of $\mathbb{F}_{97}$. ***(5 marks)***

(b) In May, Hadrian has secret key 8 and Sabina has public key 91. Find the public key of Hadrian and the shared key of Hadrian and Sabina. ***(3 marks)***

(c) Show that, in any month with chosen prime p and generator g, if the public keys of Hadrian and Sabina are inverses of each other modulo p then the secret keys h and s of Hadrian and Sabina satisfy $s \equiv -h \bmod (p-1)$ and that the shared key of Hadrian and Sabina is g^c where $c \equiv -h^2 \bmod (p-1)$. ***(4 marks)***

(d) Verify that, in (b), the public keys of Hadrian and Sabina in May are inverses of each other modulo 97 and find a positive integer c such that their shared key is 17^c. ***(3 marks)***

4 Let $\mathcal{E}$ be the elliptic curve $y^2 = x^3 + 2x + 1$ over the field $\mathbb{F}_{11}$.

(i) Find all the squares in $\mathbb{F}_{11}$. *(3 marks)*

(ii) Compute x^3 and x^3+2x+1 for each $x \in \mathbb{F}_{11}$ and hence find all the points on $\mathcal{E}$. (There are sixteen points including the point at infinity.) *(7 marks)*

(iii) Your list of points should include $(0,1)$ and $(8,1)$. Find the tangent T_1 to $\mathcal{E}$ at $(0,1)$ and identify a point $Q \neq (0,1)$ such that $Q \in T_1 \cap \mathcal{E}$. Hence, or otherwise, find $(0,1) + (0,1)$ in the group law for $\mathcal{E}$. *(4 marks)*

Find the tangent T_2 to $\mathcal{E}$ at $(8,1)$ and verify that the point $(10,8)$ is in $T_2 \cap \mathcal{E}$. Hence, or otherwise, find $(8,1) + (8,1)$ in the group law for $\mathcal{E}$. *(4 marks)*

(iv) Your list of points should include both $(10,3)$ and $(5,9)$ which are on the line L with equation $y = x + 4$. Identify a third point on $L \cap \mathcal{E}$. Hence, or otherwise, find $(10,3) + (5,9)$ in the group law for $\mathcal{E}$. *(3 marks)*

(v) It is given that $(0,1)$ has order 16 and so generates the group for $\mathcal{E}$. You wish to send the message $(5,9)$ to a member Catriona of a society that uses the ElGamal encryption method with elliptic curve $\mathcal{E}$ and generator $(0,1)$. Catriona's public key is $(8,1)$ and you choose $k = 2$ for the supplementary key. Encrypt the message in the form $((a,b),(c,d))$ where (a,b) and (c,d) are points of $\mathcal{E}$. *(4 marks)*

End of Question Paper