Durham University

EXAMINATION PAPER

Examination Session:	Year:	Exam Code:
May/June	2021	MATH3401-WE01

Title: Cryptography and Codes III

Time (for guidance only):	3 hours	
Additional Material provided:		
Materials Permitted:		
Calculators Permitted:	Yes	Models Permitted: There is no restriction on the model of calculator which may be used.

Instructions to Candidates:	Credit will be given for your answers to all questions. All questions carry the same marks. Please start each question on a new page. Please write your CIS username at the top of each page. To receive credit, your answers must show your working and explain your reasoning.

Revision:	

ED01/2021

Q1 **1.1** Using the standard convention to convert alphabetic messages into integers modulo 26, an affine cipher was used to obtain the ciphertext

$$\text{SGKXDDYUOOZDRSCDOHDCOMBOD.}$$

Find the plaintext and the key. Carefully justify your reasoning. You may assume that the plaintext is written in plain English.

1.2 Alice and Bob are using the Diffie-Hellman key exchange with $p = 269$ and a primitive root $g = 32$ to agree upon a key. Suppose the numbers exchanged between them were 41 and 53. Use this information to compute the key. Show relevant work.

1.3 Let the code $C = \langle \{ (1,2,0,0,3), (0,0,1,0,2), (0,0,0,1,4) \} \rangle \subseteq \mathbb{F}_5^5$.

i) Encode $(1,2,3) \in \mathbb{F}_5^3$ to a codeword $\boldsymbol{c}_1 \in C$.

ii) Give a generator matrix for $C^{\perp}$.

iii) Create a reduced syndrome table for C.

iv) Use your reduced syndrome table from part iii) to decode $\boldsymbol{y} = (1,4,1,1,2)$ to some codeword $\boldsymbol{c}_2 \in C$.

Q2 **2.1** Alice is using the following elliptic curve version of a Hash function to compute the hash of a message $0 \leq m < N$:

She fixes an elliptic curve E over a finite field $\mathbb{F}_p$ where p is a large prime, approximately of size $\sqrt{N}$. She fixes two points $P_1, P_2 \in E(\mathbb{F}_p)$ with orders n_1 and n_2 respectively, where $n_1 \neq n_2$ are two large primes. Alice makes $E(\mathbb{F}_p)$, P_1, P_2 and their orders n_1, n_2 public. The message $0 \leq m < N$ is further assumed to be co-prime to both n_1 and n_2. The hash function H is then defined as:

$$H(m) = [m^{-1} \bmod n_1]P_1 \oplus [m^{-1} \bmod n_2]P_2.$$

Prove that H is pre-image resistant (or one way) but not strongly collision free.

(Hint: to prove that H is pre-image resistant, relate it to solving the discrete log problem for a suitable group.)

2.2 Let $n = pq$, where p and q are odd primes such that $|p - q| < 2\sqrt{2}\sqrt[4]{n}$. Show that in this case Fermat's factorisation method takes only one step to factorise n. Justify your answer rigorously.

2.3 Let G be a cyclic group of order p^2, where p is a prime, and let P be a generator of G. Prove that solving the discrete log problem in this group, namely, given any $Q \in G$ finding $m \in \mathbb{Z}$ such that $Q = [m]P$, is equivalent to solving two discrete log problems of size p each.

Q3 **3.1** (i) Alice is using the following signature scheme to sign her messages along with the RSA encryption. Her public key is a pair (N, e) as in the RSA encryption scheme. A valid (RSA) signature on the message m satisfying $1 \leq m \leq N-1$ is an integer s with

$$s^e \equiv m \mod N.$$

Explain how Alice can produce a valid RSA signatures on a given message m, which you can assume is coprime to N. You should explain carefully why your method works.

(ii) Alice's RSA public key is $(N, e) = (413099, 7)$. She signs the message $m = 37$ with signature $s = 359779$. Without factoring N, find the signature for the message $m' = 50563$.

3.2 Let E be an elliptic curve defined over $\mathbb{Q}$ by the equation

$$y^2 = x^3 + 2p,$$

where p is a prime. Compute the torsion subgroup $E(\mathbb{Q})_{\text{tors}}$ for all possible values of the prime p. Show your work.
(Hint: Consider the cases $p = 2$ and $p \neq 2$ separately).

3.3 Alice wants to send the same secret message m to both Bob and Oscar. Suppose she has already shared $n \times n$ block cipher matrices M_1 and M_2 with Bob and Oscar respectively. The matrix M_1 is supposed to be only known to Alice and Bob (and similarly M_2 is only known to Alice and Oscar).

(i) Using the matrices M_1 and M_2, devise a way for Alice to securely send the message m to both Bob and Oscar in such a way that they cannot decipher m on their own just using their respective keys. However, Bob and Oscar can jointly figure out what m is by communicating with each other on public channels. Note that Bob and Oscar should never share their respective keys M_1 and M_2 with each other.

(ii) Suppose Alice is wary of a further issue that either Bob or Oscar could lie to the other in the above process. So she wants to further devise a way to help both Bob and Oscar verify that the message m that they obtain at the end of this process is the correct one. How can she further ensure this? For this part, you should just indicate which public key cryptosystem she can use to achieve this.

Q4 **4.1** Let S_q^n be the set of all codes of block length n over $\mathbb{F}_q$, and let $C_1 \sim_M C_2$ for $C_1,\ C_2 \in S_q^n$ mean that C_1 and C_2 are monomially equivalent. Show that $\sim_M$ is a symmetric property, that is if $C_1 \sim_M C_2$ then $C_2 \sim_M C_1$.

4.2 The check-matrix for any q-ary $[(q^r-1)/(q-1), (q^r-1)/(q-1)-r, 3]$ code is constructed in the same manner as the check-matrix of the q-ary Hamming code of redundancy r. Show, fully, that all such codes are monomially equivalent.

4.3 Let $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2+x+1)$, and let

$$H = \begin{pmatrix} 0 & 1 & 1 & x & x^2 \\ 1 & 0 & 1 & 1 & 1 \end{pmatrix} \in M_{2,5}(\mathbb{F}_4)$$

be the check matrix for a code C. Explain (in terms of the syndrome table or otherwise) why syndrome decoding to words of C is a uniquely-defined function on $\mathbb{F}_4^5$ (i.e. the syndrome table is unique up to permutation of the rows).

4.4 Let $\boldsymbol{y} = (1, x, x^2, 1, x) \in \mathbb{F}_4^5$. Decode $\boldsymbol{y}$ to a codeword $\boldsymbol{c} \in C$.

4.5 Given

$$g = \begin{pmatrix} x & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & x & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & x^2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

show that $g \in \mathrm{MAut}(C^\perp)$.

4.6 Let $\widehat{C}$ be the extended code with check matrix $\widehat{H}$, with H as in part **4.3**. If $\widehat{\boldsymbol{y}} = (1, x, x^2, 1, x, x^2) \in \mathbb{F}_4^6$, show that $d(\widehat{\boldsymbol{y}}, \widehat{\boldsymbol{c}}) > 1$ for all $\widehat{\boldsymbol{c}} \in \widehat{C}$.

Q5 **5.1** By considering punctured codes, show that the maximum number of words in a q-ary code of block length n and minimum distance d, for $d > 1$, is less than or equal to the maximum number of words in a q-ary code of block length $n-1$ and minimum distance $d-1$.

5.2 Show that the maximum number of words in a ternary code of block length 7 and minimum distance 4 is bounded from above by 27.

5.3 A code which has as many words as it is possible for a code of that block length and minimum distance to have is known as *optimal*.

Show that there exists a ternary code of block length 6 and minimum distance 3 which is both optimal and cyclic.

5.4 By considering the code generated by

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

explain why an optimal ternary code of block length 7 and minimum distance 4 has either 9 or 27 codewords.

END