FOR INTERNAL SCRUTINY (date of this version: 25/3/2026)

UNIVERSITY OF EDINBURGH

COLLEGE OF SCIENCE AND ENGINEERING

SCHOOL OF INFORMATICS

COURSE imc DATA GOES HERE!

Monday 23rd December 1963

20:00 to 23:29

INSTRUCTIONS TO CANDIDATES

1. **Note that ALL QUESTIONS ARE COMPULSORY.**
2. **DIFFERENT QUESTIONS MAY HAVE DIFFERENT NUMBERS OF TOTAL MARKS. Take note of this in allocating time to questions.**
3. **This is an OPEN BOOK examination: books, notes and other written or printed material MAY BE CONSULTED during the examination. The use of electronic devices or electronic media is NOT PERMITTED.**

Unknown Programme

Convener: ITO-Will-Determine
External Examiners: ITO-Will-Determine

THIS EXAMINATION WILL BE MARKED ANONYMOUSLY

FOR INTERNAL SCRUTINY (date of this version: 25/3/2026)

All your answers need to be justified via a formal argument.

General notation. In this exam, we use $\leftarrow$ to denote assignment of a value (e.g. $a \leftarrow b$ means that we assign the value of b to a). We use $\xleftarrow{\$}$ to denote a random sampling operation. We use $\mathsf{OR}(x)$ to denote the function computing the logical OR of all the bits of x (e.g., if $x = 010001$ then $\mathsf{OR}(x) = 1$). We use $||$ to denote the concatenation operation. We use $[x]_i^j$ to denote the function that returns the sub-bit-string of x starting from the bit in position i up to the bit in position j (e.g., if $x = 010001$ then $[x]_1^5 = 01000$). We use U_n to denote the uniform distribution of bit-strings of size n. We use $=$ to denote standard equality check and we use $\stackrel{\text{def}}{=}$ when defining an object (e.g., define how a function behaves). We use $\mathsf{negl}(n)$ to denote negligible function in n.

1. **Shift Cipher.** Alice and Bob want to exchange messages using the *Shift Cipher* as their encryption scheme. Alice is about to send a message to Bob. Eve, who is eavesdropping on their communication, knows that the message is either going to be DEMO or STOP. Describe how can Eve determine which message was sent, based on the encrypted message that she observes and explain how she can break the encryption scheme. *[3 marks]*

2. **PRF and PRG**

   (a) (PRF) Let F: $\{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a length-preserving keyed pseudorandom function (PRF). Let $H : \{0,1\}^{2n} \to \{0,1\}^n$ be a collision resistant hash function. State whether each of the following PRF candidates is or is not a pseudorandom function. If yes, prove it; if not, show a distinguisher that succeeds with non-negligible probability. Hint: to prove that some of these candidates are not PRFs, it may be useful to assume the existence of hash functions or PRFs with input and output of arbitrary size. Feel free to assume that such PRFs and hash functions do exist, and pick the length parameters that are the most suitable to prove your result.

      i. $F'(k,x) \stackrel{\text{def}}{=} H(F(k,x)||0^n)$. *[4 marks]*

      ii. $F''(k,x) \stackrel{\text{def}}{=} F(k, H(x||0^n))$ *[6 marks]*

   (b) (PRG) Let G be a pseudorandom generator (PRG) that $\{0,1\}^n \to \{0,1\}^{2n}$. State whether each of the following PRG candidates is or is not a pseudorandom generator. If yes, prove it; if not, show a distinguisher that succeeds with non-negligible probability (as for the previous exercise, if needed, you can assume that there exists PRG with input and output of arbitrary size based on your choice):

      i. $G'(x) \stackrel{\text{def}}{=} G(x)||\mathsf{OR}(x)$. *[4 marks]*

      ii. $G''(x) \stackrel{\text{def}}{=} G(x) \oplus G(x)$ *[4 marks]*

QUESTION CONTINUES ON NEXT PAGE

iii. $G'''(x) \stackrel{\text{def}}{=} G([x]_1^{n-1}||\mathsf{OR}(x))$. *[6 marks]*

3. **Hash Functions**

(a) Let $H : \{0,1\}^{2n} \to \{0,1\}^n$ be a collision resistant hash function. Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a length-preserving keyed pseudorandom function. State whether each of the following hash-function candidates is or is not a collision-resistant hash function. If yes, prove it; if not, show a distinguisher that succeeds with non-negligible probability (as before, if needed, you can assume that there exist hash functions or PRFs with input and output of arbitrary size based on your choice):

i. $H'(x) \stackrel{\text{def}}{=} F(k, x')$, where $k \leftarrow [x]_1^n$, and $x' \leftarrow [x]_{n+1}^{2n}$. *[6 marks]*

ii. $H''(x) \stackrel{\text{def}}{=} H([x]_1^{2n-1}||0)$. *[3 marks]*

4. **Public-key and secret key encryptions**

(a) Let Gen,Enc, Dec be the ElGamal encryption scheme. Let us define a new encryption scheme as follows:

- $\mathsf{Gen}'(1^n)$:
  - $pk, sk \leftarrow \mathsf{Gen}(1^n)$ (recall that $pk \stackrel{\text{def}}{=} (\mathbb{G}, q, g, g^x)$ and $sk \stackrel{\text{def}}{=} x$).
  - return (pk, sk).
- $\mathsf{Enc}'(pk, m)$:
  - Parse pk as $(\mathbb{G}, q, g, g^x)$
  - $k \leftarrow \mathbb{Z}_q$,
  - $ct \leftarrow \mathsf{Enc}(k)$
  - return $(ct, (m + k) \mod q)$
- $\mathsf{Dec}'(sk, (ct, t))$:
  - $\alpha \leftarrow \mathsf{Dec}(sk, ct)$
  - return $(t - \alpha) \mod q$

Prove that the above encryption scheme $(\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ is IND-CPA secure. Hint: to prove the security of the scheme you can refer to results that we have proven in the class. In particular, you can use the fact that ElGamal is CPA secure. *[5 marks]*

(b) Let Π with $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a secret key CCA secure encryption scheme. Design a CPA secure scheme that is not CCA secure. For this exercise, you *cannot* use additional computational cryptographic primitives like PRGs, PRFs or CPA encryption scheme (of course), but you can (and should) use the algorithms of Π. Other than that, you can use any type of operation, like bit-string operation (e.g., xor) and the ability to sample random strings. *[6 marks]*

5. **Digital Signatures.** Let $Sig \stackrel{\text{def}}{=} (\mathsf{Sign}, \mathsf{Verify})$ be a secure digital signature scheme. Prove or disprove the security of the following digital signature scheme $Sig' \stackrel{\text{def}}{=} (\mathsf{Sign}', \mathsf{Verify}')$. *[3 marks]*

$\mathsf{Sign}'(sk, m)$:
  $\theta \leftarrow \mathsf{Sign}(sk, [m]_1^{n-1})$
  Return θ

$\mathsf{Verify}'(pk, m, \theta)$:
  Return $\mathsf{Verify}(pk, [m]_1^{n-1}, \theta)$