UNIVERSITY OF BRISTOL

JANUARY 2014 Examination Period

FACULTY OF ENGINEERING

Examination for the Degree of
Bachelor and Master of Engineering and Bachelor and Master of Science

COMS30002J
CRYPTOGRAPHY A

TIME ALLOWED:
2 Hours

This paper contains *four* questions.
All answers will be used for assessment.
The maximum for this paper is *60 marks*.

Other Instructions:

1. Calculators must have the Faculty of Engineering Seal of Approval.

TURN OVER ONLY WHEN TOLD TO START WRITING

Q1. This question focuses on the Damgård ElGamal encryption scheme, which is a variation on the original ElGamal scheme. The scheme is defined as follows:

Key generation Kg generates a cyclic group G_q of prime order q with generator g. A private decryption key sk consists of two elements $x, \omega \in \mathbb{Z}_q$ both sampled independently and uniformly at random. The public key consists of the group description (G_q, q, g) together with the group elements $h \leftarrow g^\omega$ and $y \leftarrow g^x$.

Encryption Enc takes as input a public key pk and a message $\mathsf{m} \in \mathsf{G}_q$, uniformly at random selects r from $\mathbb{Z}_q$ and computes the ciphertext $c \leftarrow (g^r, h^r, m \cdot y^r)$.

Decryption Dec takes as input a private key sk and a ciphertext $c = (c_1, c_2, c_3)$. It checks whether $c_1^\omega = c_2$ and if and only if this is the case, it returns $m' \leftarrow c_3 c_1^{-x}$.

(a) Prove the correctness of the scheme.

[4 marks]

(b) The scheme is malleable. Explain what malleability means in general, demonstrate the malleability of this scheme, and comment on the implications in terms of security.

[4 marks]

(c) This scheme is derived from ElGamal. Explain how Damgård ElGamal differs from ElGamal.

[4 marks]

(d) ElGamal itself can be shown to be IND-CPA secure under the DDH assumption. Give the definition of IND-CPA security.

[3 marks]

(e) Prove that if ElGamal is IND-CPA secure, then so is Damgård ElGamal.

[5 marks]

Q2. This question focuses on building a message authentication code from an authenticated encryption scheme. To this end, let $(\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec})$ be an authenticated encryption scheme and consider the MAC scheme $(\mathsf{Kg}, \mathsf{Tag}, \mathsf{Vrfy})$ where key generation Kg for the MAC scheme is exactly the same as that of the authenticated encryption scheme, and

Tagging Tag takes as input a key k and a message m. It computes $\tau \leftarrow \mathsf{Enc}(\mathsf{k}, \mathsf{m})$.

Verification Vrfy takes as input a k, a message m, and a tag τ. It computes $\mathsf{m}' \leftarrow \mathsf{Dec}(\mathsf{k}, \tau)$ and accepts iff $\mathsf{m}' = \mathsf{m}$.

(a) Prove the correctness of the MAC scheme, assuming correctness of the authenticated encryption scheme.

[2 marks]

(b) Comment on the efficiency and tag size of the MAC scheme.

[2 marks]

(c) Katz and Lindell gave three principles of modern cryptology. Name these principles (no explanation needed) and identify each of these principles in the statement:

The MAC scheme is existentially unforgeable under chosen message attacks (EUF-CMA secure) if the underlying authenticated encryption scheme satifies integrity of ciphertext (INT-CTXT secure).

[4 marks]

(d) Give the definition of EUF-CMA security for a MAC scheme.

[3 marks]

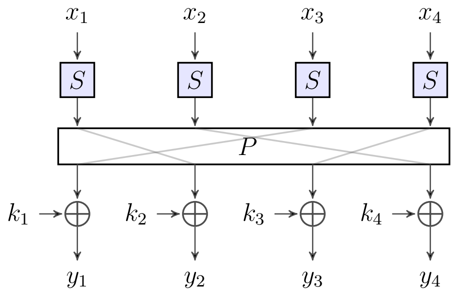
(e) Compare the definition of INT-CTXT security for a symmetric encryption scheme with that of EUF-CMA security for MACs: what are the differences and what are the similarities?

[5 marks]

(f) Consider the MAC scheme as described above, but where the verification routine is changed as follows: Vrfy' takes as input a k, a message m, and a tag τ. It computes $\mathsf{m}' \leftarrow \mathsf{Dec}(\mathsf{k}, \tau)$ and accepts iff $\mathsf{m}' \neq \perp$. How does this modification affect security? Argue your answer.

[3 marks]

Q3. This question focuses on substitution-permutation networks. These are commonly used to build blockciphers. A blockcipher typically consists of several rounds of an SP network, with S and P fixed and the various round keys generated from the master key using some key schedule. Below is an illustration of a single round of an SP-network.



(a) What is a blockcipher and what is meant by its block-length? *[2 marks]*

(b) Explain Kerckhoffs's principle in terms of a blockcipher built from an SP-network. What are the implications on the block-length and the key-length when a security level of 128-bit is desired (assuming a single round-key uniquely determines the overall blockcipher key)? *[3 marks]*

(c) One round (as depicted above) is insufficient as a blockcipher. Give an attack that is strong yet efficient, and describe what kind of attack it is. *[3 marks]*

(d) Why is omitting the S-boxes (from a multi-round SP-network) a bad idea? *[3 marks]*

Q4. This question focuses on a family of RSA-inspired signature schemes, defined as follows:

Key generation Kg selects 1023-bit prime numbers p' and q' such that $p \leftarrow 2p' + 1$ and $q \leftarrow 2q' + 1$ are both prime as well. Let $N \leftarrow pq$. Denote with Q_N the group of quadratic residues modulo N, that is $x \in Q_N$ iff $x \in \mathbb{Z}_N^*$ and there is some $y \in \mathbb{Z}_n$ such that $x \equiv y^2 \bmod N$. Key generation also selects a function f from the message space into Q_N (how this function is selected is immaterial to this question). The public key consists of N and the function f; the private key is (p', q').

Signing Sign takes as input a private key and a message m. It computes $y \in Q_N$ and e some 128-bit prime number such that $y^e = f(\mathsf{m}) \bmod N$. The signature is the pair (y, e).

Verification Vrfy takes as input a public key $\mathsf{pk} = (N, f)$, a message m, and a purported signature (y, e). It accepts iff $y^e = f(\mathsf{m}) \bmod N$.

(a) Show how to implement the signing algorithm, i.e. describe an efficient algorithm to compute the signature (y, e) using knowledge of the private key. You may assume an efficient routine $\mathrm{GenPrime}$ that on input ℓ outputs a random prime of length ℓ. *[4 marks]*

(b) Argue why your algorithm is efficient. *[3 marks]*

(c) Argue why your algorithm is correct, namely that the signatures that are generated will pass verification. *[3 marks]*

END OF PAPER

UNIVERSITY OF BRISTOL

JANUARY 2015 Examination Period

FACULTY OF ENGINEERING

Examination for the Degree of
Bachelor and Master of Engineering and Bachelor and Master of Science

COMS-30002(J)
CRYPTOGRAPHY A

TIME ALLOWED:
2 Hours

This paper contains *four* questions.
All answers will be used for assessment.
The maximum for this paper is *60 marks*.

Other Instructions:

1. Calculators must have the Faculty of Engineering Seal of Approval.

TURN OVER ONLY WHEN TOLD TO START WRITING

Q1. For each of the following statements decide whether it is true or false, and write down in the exam book the correct answer. Provide a short justification for each answer.

(a) The One-Time Pad is malleable.

[3 marks]

(b) CBC mode is OW-CCA secure.

[3 marks]

(c) Any probabilistic symmetric key encryption scheme is IND-CPA secure.

[3 marks]

(d) A deterministic symmetric key encryption scheme cannot be OW-CCA secure.

[3 marks]

(e) A homomorphic public key encryption scheme cannot be OW-CCA secure.

[3 marks]

Q2. This question focuses on the relationship between symmetric and public key primitives.

Let $(\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec})$ be a public key encryption scheme. Consider the symmetric key encryption scheme $(\mathsf{Kg}', \mathsf{Enc}', \mathsf{Dec}')$ that works as follows:

Key generation Kg' runs $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Kg}$ and returns the pair $(\mathsf{pk}, \mathsf{sk})$ as the symmetric key k.

Encryption Enc' takes as input the symmetric key $\mathsf{k} = (\mathsf{pk}, \mathsf{sk})$ and a message m and returns $\mathsf{Enc}_{\mathsf{pk}}(\mathsf{m})$.

Decryption Dec' takes as input the symmetric key $\mathsf{k} = (\mathsf{pk}, \mathsf{sk})$ and a ciphertext c and returns $\mathsf{Dec}_{\mathsf{sk}}(c)$.

(a) Describe the IND-CCA security notion for symmetric encryption schemes.

[3 marks]

(b) Which oracle is missing from the IND-CCA security notion of public key schemes and why?

[2 marks]

(c) Prove that if the public key scheme $(\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec})$ is IND-CCA secure, then so is the resulting symmetric scheme $(\mathsf{Kg}', \mathsf{Enc}', \mathsf{Dec}')$.

[5 marks]

(d) Show that if for some public key scheme $(\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec})$, the resulting symmetric scheme $(\mathsf{Kg}', \mathsf{Enc}', \mathsf{Dec}')$ is IND-CCA secure, this does not imply that the original public key scheme is IND-CCA secure.

[5 marks]

Q3. This question focuses on signature schemes and the related use of hash functions.

(a) Give the generic syntax of a signature scheme (in the standard model) by describing which algorithms are involved and what their general input/output behaviour is. Also include the appropriate correctness requirement.

[4 marks]

(b) Describe the security model which should be satisfied by an EUF-CMA secure scheme in the standard model by giving a diagram depicting the relevant security game together with an informal explanation (in words).

[3 marks]

(c) The hash-then-sign paradigm can be used to extend the domain of a signature scheme. Given a signature scheme with domain $\{0,1\}^n$ and an arbitrary hash function $H : \{0,1\}^{2n} \rightarrow \{0,1\}^n$, the corresponding hash-then-sign signature scheme can sign messages in $\{0,1\}^{2n}$. Describe how the hash-then-sign scheme works by specifying the relevant algorithms.

[3 marks]

(d) Consider the hash function $H : \{0,1\}^{2n} \rightarrow \{0,1\}^n$ defined by $H(x_0||x_1) = x_0 \oplus x_1$ (that is, the input to H is split in two equal parts that are subsequently xored together). Evaluate the security of the resulting hash-then-sign scheme.

[5 marks]

Q4. This question addresses a cryptosystem using ideas from both RSA and ElGamal.

Key generation Kg randomly generates distinct primes p', q' such that $p \leftarrow 2p' + 1$ and $q \leftarrow 2q' + 1$ are prime as well. Set $N \leftarrow pq$ and let Q_N denote the group of quadratic residues modulo N, thus $z \in Q_N$ iff $z \in \mathbb{Z}_N{}^*$ and there exists a $w \in \mathbb{Z}_N{}^*$ such that $z = w^2 \bmod N$. Pick a generator g of Q_N; both g and Q_N have order $p'q'$. Select private exponent $x \in \mathbb{Z}_q$ and compute $y \leftarrow g^x \bmod N$. The public key comprises $\mathsf{pk} = (g, y, N)$ and the private key $\mathsf{sk} = (x, p', q')$.

Encryption Enc takes as input a public key $\mathsf{pk} = (g, y, N)$ and a message $m \in Q_N$. It randomly selects $r \in \mathbb{Z}_{N^2}$ and computes $c_1 \leftarrow g^r \bmod N$ and $c_2 \leftarrow m \cdot y^r \bmod N$. The ciphertext is (c_1, c_2).

Decryption Dec takes as input a private key $\mathsf{sk} = (x, p', q')$ and a ciphertext (c_1, c_2). It computes and returns $m' \leftarrow c_2 \cdot c_1^{p'q'-x} \bmod N$.

(a) Prove correctness of the cryptosystem as described above.

[5 marks]

(b) Give a detailed explanation how to exploit the Chinese Remainder Theorem for efficient decryption. How could you store the private key redundantly to facilitate this speed up?

[5 marks]

(c) Using your knowledge of both the RSA and the ElGamal cryptosystems, argue about the (in)security of the RSA-ElGamal cryptosystem. Make at least one positive and one negative observation.

[5 marks]

END OF PAPER

UNIVERSITY OF BRISTOL

JANUARY 2016 Examination Period

FACULTY OF ENGINEERING

Examination for the Degree of
Bachelor and Master of Engineering and Bachelor and Master of Science

COMS-30002(J)
CRYPTOGRAPHY A

TIME ALLOWED:
2 Hours

This paper contains *four* questions.
All answers will be used for assessment.
The maximum for this paper is *60 marks*.

Other Instructions:

1. Calculators must have the Faculty of Engineering Seal of Approval.

TURN OVER ONLY WHEN TOLD TO START WRITING

Q1. For each of the following statements decide whether it is true or false, and write down the correct answer in the exam book. Provide a short justification for each answer.

(a) Perfect secrecy of the One-Time Pad implies that the key can be reused securely.

[3 marks]

(b) CTR mode using AES-128 is IND-CCA secure.

[3 marks]

(c) A single round of the Feistel construction does not suffice for a secure blockcipher.

[3 marks]

(d) For a *deterministic* public key encryption scheme, OW-CCA security does not imply OW-CPA security.

[3 marks]

(e) Cryptology is not used in practice.

[3 marks]

Q2. This question focuses on a variant of the RSA cryptosystem.

Key generation Kg selects three random yet distinct 767-bit prime numbers p', q', and r' such that $p \leftarrow 2p' + 1, q \leftarrow 2q' + 1$, and $r \leftarrow 2r' + 1$ are all prime as well. Let $N \leftarrow p \cdot q \cdot r$. Set $e \leftarrow 3$ and set d to the smallest positive integer such that the least common multiple $\mathrm{lcm}(p - 1, q - 1, r - 1)$ divides $d \cdot e - 1$. Publish (N, e) as the public key pk and keep (N, d) as the private key sk.

Encryption Enc takes as input the public key $\mathsf{pk} = (N, e)$ and a message $\mathsf{m} \in \mathbb{Z}_N$. It computes and returns ciphertext $\mathsf{c} \leftarrow \mathsf{m}^e \bmod N$.

Decryption Dec takes as input a private key $\mathsf{sk} = (N, d)$ and a ciphertext $\mathsf{c} \in \mathbb{Z}_N$. It computes and returns $\mathsf{m}' \leftarrow \mathsf{c}^d \bmod N$.

(a) Prove correctness of the scheme.

[5 marks]

(b) Discuss the strengths and weaknesses of the encryption scheme. Mention at least three distinct ones (strengths and weaknesses combined). Illustrate with attacks where appropriate (no reductions are required).

[5 marks]

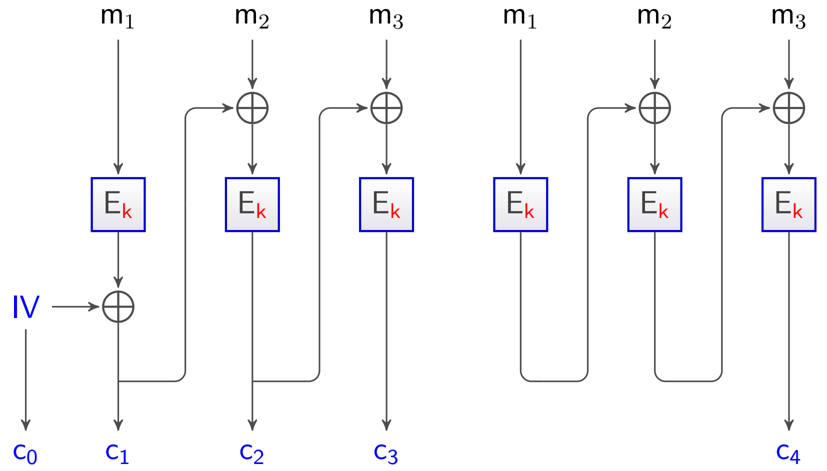
(c) Describe how you would build an EUF-CMA signature scheme related to this encryption scheme by specifying the relevant algorithms for key generation, signing, and verification.

[3 marks]

(d) Under what assumption(s) would your signature scheme be EUF-CMA secure (no reduction required)?

[2 marks]

Q3. This question asks you to evaluate the security of an authenticated encryption scheme. The scheme is based on combining CBC-style encryption and authentication, both based on DES. Let E denote the encryption algorithm of the DES blockcipher. For key generation, generate a single DES key k that will be used throughout. To encrypt a three block message $(\mathsf{m}_1, \mathsf{m}_2, \mathsf{m}_3)$, generate a random initial vector IV and output the ciphertext $(\mathsf{c}_0, \ldots, \mathsf{c}_4)$ with the computation according to the diagram below. Here the final block of ciphertext c_4 is used as an authentication tag. The scheme generalizes to messages of an arbitrary number of blocks in the natural way.



(a) Describe what decryption would look like for this scheme. Base your decryption algorithm on ciphertexts corresponding to 3-block messages (as above).

[3 marks]

(b) Point out as many dubious design decisions of the scheme as you can. For each shortcoming, you should identify as clearly as possible which part of the scheme you are referring to, explain how and why security (or efficiency) suffers by presenting attacks (or referring to taught material), and suggest a remedy. You can obtain up to four points per shortcoming.

[12 marks]

Q4. This question addresses an ElGamal-like cryptosystem. Assume G_q is a given group of (known) prime order q with public generator g. Consider the following algorithms defining key generation and encryption of the EGL cryptosystem.

Key generation Kg randomly generates a second generator f and selects two exponents x_1 and x_2 uniformly at random from $\mathbb{Z}_q$. Compute $y \leftarrow f^{x_1} g^{x_2}$. The public key comprises $\mathsf{pk} = (f, y)$ and the private key $\mathsf{sk} = (x_1, x_2)$.

Encryption Enc takes as input a public key $\mathsf{pk} = (f, y)$ and a message $m \in \mathsf{G}_q$. It randomly selects $r \in \mathbb{Z}_q$ and computes $c_1 \leftarrow f^r, c_2 \leftarrow g^r$ and $c_3 \leftarrow m \cdot y^r$. The ciphertext is (c_1, c_2, c_3).

(a) Describe a suitable decryption algorithm for the EGL cryptosystem.

[3 marks]

(b) Show that the EGL cryptosystem is homomorphic.

[2 marks]

(c) Under an appropriate assumption, either show that the EGL cryptosystem is OW-CPA or IND-CPA secure (your choice; both are possible). Clearly describe both the security notion and the assumption and explain how you set up your reduction, before fleshing out the details.

[10 marks]

END OF PAPER

UNIVERSITY OF BRISTOL

JANUARY 2017 Examination Period

FACULTY OF ENGINEERING

Examination for the Degree of
Bachelor and Master of Engineering and Bachelor and Master of Science

COMS-30002(J)
CRYPTOGRAPHY A

TIME ALLOWED:
2 Hours

This paper contains *three* questions.
All answers will be used for assessment.
The maximum for this paper is *60 marks*.

Other Instructions:

1. Calculators must have the Faculty of Engineering Seal of Approval.

TURN OVER ONLY WHEN TOLD TO START WRITING

Q1. (a) A friend of yours has stumbled over the concept of the one-time pad. Unfortunately, he did not attend Crypto A, so he needs your help to make sense of the following statements. Moreover, some of the statements are misleading or even incorrect. Comment on the validity of each of the statements below, drawing particular attention to mistakes or misleading claims.

[12 marks]

A. the one time pad is useless because it just xors plaintexts and ciphertexts.

B. the one time pad provides perfect secrecy, and hence the key can be reused securely.

C. the one time pad is not secure because the key needs to be as long as the message that you encrypt.

D. the one time pad is so secure that even an adversary with unlimited computing power cannot break it.

E. the one time pad provides perfect secrecy and hence integrity of ciphertexts.

(b) Your friend has moved on to more modern cryptology, but is still struggling. He has realized that key lengths are important when implementing cryptography in real life, but isn't entirely sure about the following four statements. Again, comment on each of the statements below, drawing particular attention to mistakes or misleading ones.

[6 marks]

A. The longer the key the more secure any system will be.

B. Furthermore, it is important to have a good random number generator for key generation.

C. However, in case of public key cryptography, it is o.k. to have short public keys.

D. Even if you loose your secret key, you can still decrypt messages.

Q2. WhatsApp is a messaging service that introduced end-to-end encryption in 2016. There is a WhatsApp Security Whitepaper that explains how media and other attachments are transmitted. There are various steps to ensure that both the sender and receiver share two keys, namely an AES256 key and a HMAC-SHA256 key. With these in place, the main cryptographic step reads:

> The sender encrypts the attachment with the AES256 key in CBC mode with a random IV, then appends a MAC of the ciphertext using HMAC-SHA256.

(a) Unpack the terminology from the quote above by explaining what the various abbreviations (AES256, CBC, IV, MAC, HMAC, SHA256) refer to and what their general purpose is. You do not (yet) have to explain how they work.

[12 marks]

(b) For *one* of the schemes or modes mentioned (AES256, CBC, HMAC, SHA256) explain at a high level how it works.

[3 marks]

(c) Assume a receiver already has all the relevant keys. How would they decrypt some received ciphertext? (Note: describe the steps in roughly the same amount of detail as in the quote above.)

[3 marks]

(d) What security goal(s) do you think WhatsApp is targeting? Describe the goal informally and link it to a formal security notion (you do not need to give the full definition or diagram of the security notion).

[4 marks]

Q3. This question addresses RSA-OAEP and a simplification thereof. Let's first consider the original.

(a) Explain the purpose of the original OAEP. In particular, which weaknesses of vanilla or textbook RSA are addressed by using RSA-OAEP instead?

[3 marks]

(b) RSA-OAEP can be proven IND-CCA secure under the RSA assumption in the random oracle model. Prove that any IND-CCA secure public key encryption scheme is also OW-CPA secure (you may ignore the random oracle).

[6 marks]

Now consider the following simplified version of RSA-OAEP instead. Let H be a public hash function from $\{0,1\}^{1535} \to \{0,1\}^{512}$ and, given an RSA modulus N and some $R \in \{0,1\}^{128}$, define $\mathsf{pad}_R : \{0,1\}^{512} \to \mathbb{Z}_N$ by $\mathsf{pad}_R(\mathsf{m}) = (0^{1407}||R||\mathsf{H}(0^{1407}||R) \oplus \mathsf{m})$ where this 2047-bit string is interpreted as an integer in $\{0, ...2^{2047} - 1\} \subset \mathbb{Z}_N$ (for instance, the bitstring $(0^{2045}||11)$ corresponds to 3).

Key generation Kg selects two random yet distinct 1024-bit prime numbers p and q, both congruent to 2 modulo 3. Let $N \leftarrow p \cdot q$ and $e \leftarrow 3$. Set d to the inverse of e modulo $\phi(N)$. Select a random $R \in \{0,1\}^{128}$ and publish (N, R, e) as the public key pk while keeping (N, R, d) as the private key sk.

Encryption Enc takes as input the public key $\mathsf{pk} = (N, R, e)$ and a message $\mathsf{m} \in \{0,1\}^{512}$. It computes and returns ciphertext $\mathsf{c} \leftarrow \mathsf{pad}_R(\mathsf{m})^e \bmod N$.

(c) Describe how decryption for the RSA version with padding as above works.

[2 marks]

(d) Explain why decryption, as described by you, works. Concentrate on the modular arithmetic involved.

[3 marks]

(e) Assume H is a secure hash function. Argue about the security of the scheme above. Highlighting multiple strengths and weaknesses may result in higher marks. Where possible, illustrate a weakness by giving an explicit attack.

[6 marks]

END OF PAPER

UNIVERSITY OF BRISTOL

JANUARY 2018 Examination Period

FACULTY OF ENGINEERING

Examination for the Degree of
Bachelor and Master of Engineering and Bachelor and Master of Science

COMS-30002(J)
CRYPTOGRAPHY A

TIME ALLOWED:
2 Hours

This paper contains *three* questions.
All answers will be used for assessment.
The maximum for this paper is *50 marks*.

Other Instructions:

1. Calculators must have the Faculty of Engineering Seal of Approval.

TURN OVER ONLY WHEN TOLD TO START WRITING

Q1. For each of the questions below, four possible answers are presented. Select *all* the answers that you believe apply, or write "none" if you believe none apply. You do not need to justify your answer.

For each question, you can receive up to 3 points, with 3 points only for the perfect answer and one point deducted per incorrect classification, to a minimum of 0 points per question (e.g. if the correct answer is "A and B" then answering "B" leads to 2 points, whereas answering "B and C" only leads to 1 point).

[15 marks]

(a) Which of the following modes most closely mirrors the one-time pad?

A. CTR
B. CBC
C. CFB
D. OFB

(b) Which of the following statements is accurate?

A. AES is an SP Network
B. AES is a Feistel cipher
C. AES is an iterated cipher
D. AES uses key-whitening

(c) In the sentences below, "harder than" should be interpreted as "known to be equally hard as or strictly harder than".

A. Solving the DDH problem is harder than solving DLP
B. Solving the DDH problem is harder than solving the CDH problem
C. Solving the CDH problem is harder than solving DLP
D. Solving DLP is harder than solving the DDH problem.

(d) Which of the following schemes are homomorphic?

A. Vanilla ElGamal
B. Vanilla RSA Encryption
C. RSA-OAEP
D. Hybrid ElGamal

(e) The Chinese Remainder Theorem is commonly used to speed up

A. RSA encryption
B. RSA decryption
C. ElGamal encryption
D. ElGamal decryption

Q2. The one-time pad can be proven to be perfectly secret.

(a) Describe the three algorithms Kg, Enc, and Dec of the one-time pad.

[3 marks]

(b) Give the definition of perfect secrecy as a formal, probabilistic statement and describe in words what that statement intuitively captures.

[3 marks]

(c) There is an equivalent formalisation of perfect secrecy. Provide that statement and its intuitive meaning.

[2 marks]

(d) The one-time pad is seldom used directly and on its own in practice, say for secure e-mail. Why is this?

[5 marks]

(e) Imagine that one would create OTP-MAC in a similar way to CBC-MAC, by encrypting a message of arbitrary length and outputting the final 128 bits (padded with zeroes if needed) as the tag. Why is this OTP-MAC a bad idea?

[2 marks]

Q3. Schnorr signatures are a way of creating signature scheme based on the discrete logarithm problem in Schnorr subgroups of $\mathbb{Z}_p^*$. Key generation and signing work as follows.

Key generation Kg Selects random 2048-bit p and 256-bit q prime numbers such that q divides $p-1$. It selects a random element $g \in \mathbb{Z}_p^*$ of order q. Let $\mathsf{G}_q \subseteq \mathbb{Z}_p^*$ be the group of order q generated by g and let $\mathsf{H} : \mathsf{G}_q \times \{0,1\}^* \to \mathbb{Z}_q$ be a hash function.

Finally, it selects a random exponent $x \in \mathbb{Z}_q$ and sets $h \leftarrow g^x \bmod p$. Publish (p, q, g, h, H) as the verification key vk and keep (p, q, g, x, H) as the private signing key sk.

Signing Sign Takes as input the private signing key $\mathsf{sk} = (p, q, g, x, \mathsf{H})$ and a message $m \in \{0,1\}^*$. It selects a random element $w \in \mathbb{Z}_q$ and sets $a \leftarrow g^w \bmod p$ followed by $c \leftarrow \mathsf{H}(a, m)$. Set $r \leftarrow w - cx \bmod q$. Return (c, r) as the signature on m.

With a suitable verification algorithm, Schnorr signatures can be proven secure—for some relevant notion of security—in the random oracle model based on the discrete logarithm problem.

(a) State the discrete logarithm problem.

[2 marks]

(b) Describe and motivate a relevant security notion for signature schemes.

[6 marks]

(c) In the security reduction, what component of the signature scheme would be modelled by the random oracle?

[1 mark]

(d) Describe a suitable verification algorithm (hint: recompute a).

[3 marks]

For a chosen-prefix preimage attack against the hash function H, an adversary is given a target digest $z \in \mathbb{Z}_q$ and target prefix $a \in \mathsf{G}_q$, and has to find an m such that $z = \mathsf{H}(a, m)$.

(e) Prove that if H is collision resistant, then it is also resistant against chosen-prefix preimage attacks.

[4 marks]

(f) Show how susceptibility of H against chosen-prefix preimage attacks leads to a vulnerability against the signature scheme; name the attack against the signature scheme as precisely as possible.

[4 marks]

END OF PAPER

UNIVERSITY OF BRISTOL

January 2020 Examination Period

FACULTY OF ENGINEERING

Third Year Examination for the Degrees of
Bachelor of Science and Master of Engineering

COMS-30002(J)
Cryptography A

TIME ALLOWED:
2 Hours

This paper contains four questions.
All answers will be used for assessment.
The maximum for this paper is 50 marks.

PLEASE WRITE YOUR 7 DIGIT STUDENT NUMBER (NOT CANDIDATE NUMBER) ON THE ANSWER BOOKLET. YOUR STUDENT NUMBER CAN BE FOUND ON YOUR UCARD

Other Instructions:

1. Calculators must have the Faculty of Engineering Seal of Approval.

TURN OVER ONLY WHEN TOLD TO START WRITING

Q1. For each of the questions below, four possible answers are presented. Zero or more of these answers are correct. Select all the answers that you believe apply, or write ”none” if you believe none apply. You do not need to justify your answer.

Each question carries 3 marks. You lose one mark for each incorrect classification, down to a minimum of 0 marks per question. (For example, if the correct answer is ”A and B”, then answering ”B”, or ”none” leads to 2 points, whereas answering ”B and C” only leads to 1 point.) No marks will be awarded for questions to which you give no answer, so do make sure to write ”none” in case you believe none of the proposed answers apply.

(a) Which of these statements apply to the one-time pad?

A. The one-time pad provides perfect secrecy.

B. The one-time pad is not secure if keys are reused.

C. The one-time pad is always secure, however it is used.

D. The one-time pad is secure even when there are more messages than possible keys.

[3 marks]

(b) Which of these statements apply to Encrypt-then-MAC?

A. Encrypt-then-MAC is a blockcipher construction.

B. One needs to be careful to include both the nonce and ciphertext in the MAC computation.

C. If Encrypt is IND-secure and MAC is EUF-CMA-secure, then Encrypt-then-MAC is AE secure.

D. If Encrypt is IND-secure and MAC is EUF-CMA-secure, then Encrypt-then-MAC is IND-CCA secure.

[3 marks]

(c) Which of the following statements most accurately reflect the threat quantum computers pose to modern cryptography?

A. Grover’s algorithm allows a quantum computer to factor or compute discrete logarithms in time polynomial in the bitsize of the input.

B. Grover’s quantum search algorithm speeds exhaustive search attacks on symmetric cryptography from $\mathcal{O}(N)$ to $\mathcal{O}(\sqrt{N})$.

C. Grover’s and Shor’s algorithms are known to be the only possible threats that would arise from a scalable quantum computer.

D. Shor’s period-finding algorithm allows a quantum computer to factor or compute discrete logarithms in time polynomial in the bitsize of the input.

[3 marks]

(d) For which of the following choices for $f(x) \in \mathbb{Z}/3\mathbb{Z}[x]$ is $(\mathbb{Z}/3\mathbb{Z})[x]/(f(x))$ a field?

A. $f(x) = x^2 + 1$.

B. $f(x) = x^4 + 2 * x^2 + 1$.

C. $f(x) = x^2 - 1$.

D. $f(x) = x^3 + x + 1$.

[3 marks]

(e) If you are trying to solve a discrete logarithm problem in a large prime-order subgroup of a finite field $\mathbb{F}_p$, which of the following algorithms are likely to be most efficient (disregarding memory concerns)?

A. Index calculus

B. Pollard-rho

C. Baby-step-giant-step

D. Pohlig-Hellman

[3 marks]

Q2. In this question, we will consider a candidate authenticated encryption scheme, shown below, where E_K is a blockcipher that we assume is IND-secure. We only define this scheme for messages whose length is exactly three times the block length ℓ of the underlying blockcipher.

```
$\mathsf{Enc}_K^N(M = M[1] \| M[2] \| M[3])$
$C[0] \leftarrow N$
for $i \in [1, \ldots, 3]$
   $X[i] \leftarrow \mathsf{E}_K(C[i-1])$
   $C[i] \leftarrow M[i] \oplus X[i]$
$K' \leftarrow \mathsf{E}_K(N)$
$T \leftarrow C[n] \oplus K'$
return $(C[1] \| C[2] \| C[3], T)$
```

(a) Which mode of operation is the blockcipher being used in?

[2 marks]

(b) Describe, draw or define the decryption oracle, taking care to process as little unverified data as possible.

[3 marks]

(c) We would like to prove that our candidate scheme is a secure authenticated encryption scheme. This first requires us to prove that the scheme is a secure (nonce-based) encryption scheme. Define an adversary's advantage in breaking a scheme's indistinguishability. This must include a description (in words, diagram or code) of an experiment.

[3 marks]

(d) Our candidate scheme does not provide (nonce-based) indistinguishability. Name (or describe) a weaker indistinguishability notion that is likely to hold on our candidate scheme. Give a rough argument explaining why you believe this weaker notion applies to our scheme.

[3 marks]

(e) Does the scheme provide ciphertext integrity? If yes, explain why informally and explain the high-level reduction logic (without writing out the reduction or analyzing it). If no, demonstrate an attack and identify what kind of attack it is.

[4 marks]

Q3. (a) If p is a prime and $a \in \mathbb{Z}_{>0}$, state the conditions on $f(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$ in order for $(\mathbb{Z}/p\mathbb{Z})[x]/(f(x))$ to be a field of size p^a.

[1 mark]

(b) Given a polynomial $g(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ and $m \in \mathbb{Z}_{\geq 2}$, define $g(x) \bmod m$ to be

$$g(x) \bmod m := \sum_{i=0}^{n} (a_i \bmod m) x^i \in (\mathbb{Z}/m\mathbb{Z})[x].$$

Give a polynomial $g(x) \in \mathbb{Z}[x]$ such that $(\mathbb{Z}/2\mathbb{Z})[x]/(g(x) \bmod 2)$ is a finite field of size 4, but $(\mathbb{Z}/3\mathbb{Z})[x]/(g(x) \bmod 3)$ is not a field. Justify your answer.

[4 marks]

Q4. In this question, we will play the part of an adversary and use index calculus to break the discrete logarithm problem to compute Alice's private key and forge her digital signature. It is recommended that you use a calculator to help you. Suppose that Alice is using a service which requires ElGamal signatures. This service uses the finite field $\mathbb{F}_{107}$ and the generator $g = 17$ for the unit group of the finite field $\mathbb{F}_{107}^*$. (The generator 17 has order 106 so does indeed generate the whole group).

(a) Using the following equations:

$$17^2 \equiv 3 \cdot 5^2 \pmod{107}$$
$$17^9 \equiv 2^2 \cdot 5 \pmod{107}$$
$$17^{11} \equiv 2 \pmod{107},$$

compute $\log_{17}(2)$, $\log_{17}(3)$, and $\log_{17}(5)$ mod 106.

[4 marks]

(b) Alice chooses a secret $a \in \mathbb{Z} \pmod{106}$ and publishes her public key $17^a = 94 \pmod{107}$. Find Alice's secret using index calculus with factor base $\{2, 3, 5\}$.

[3 marks]

(c) Give the steps of signing and verifying a message using ElGamal.

[4 marks]

(d) Using the nonce $k = 1$ and a message m with hash $H(m) = 0$, compute an ElGamal signature as if you were Alice. (If you did not manage part (b), suppose for this question that Alice's secret was $a = 102$. This is not the correct answer to (b).)

[2 marks]

(e) Suppose now that you observe Alice and Bob using the same parameters to compute a shared secret via a Diffie-Hellman key exchange. Bob's public key is $17^b = 54 \pmod{107}$. Compute their shared secret. (Hint: observe that $54 = 2^{-1} \pmod{107}$.)

[2 marks]

END OF PAPER

UNIVERSITY OF BRISTOL

January 2022

Faculty of Engineering

Examination for the Degrees
of
Bachelor of Science
Master of Engineering
Master of Science

COMS30021(J)
Cryptology

TIME ALLOWED:
3 Hours

This paper contains 6 questions over 11 pages.
Answer all the questions.
The maximum for this paper is 100 marks.

Other Instructions

1. This is an open book exam.
2. Automated and programmable computing devices are permitted.
3. After completion of this exam, you will have 30 minutes to upload your submission to Blackboard.

Preamble

This exam is composed of 6 questions, *all* of which you must answer:

- 2 regarding *symmetric cryptography*;

Question	Points
Symmetric Cryptography — MAQs	30
Message Authentication Codes	10
Total:	40

- 1 at the interface between symmetric and asymmetric cryptography; and

Question	Points
Security Notions for Digital Signatures	10
Total:	10

- 3 regarding *asymmetric cryptography*.

Question	Points
Asymmetric Cryptography — MAQs	12
Key-exchange and digital signatures	21
Cryptanalysis of the Discrete Logarithm Problem	17
Total:	50

Use of calculators. You are free to use a computer or calculator throughout, but *must* show your working where specified. Wolfram Alpha[1]is sufficient for most of the questions in this exam (at least those that are made easier by having access to a calculator), but feel free to use other tools.

Open Book and Referencing. This is an open book exam conducted online. If you reference external material (material that we did not provide during the course of the unit), you *must* include clear references, in line with the University's academic integrity policy.

[1] https://www.wolframalpha.com/

Marking MAQs. Multiple Answer Questions (in Questions 1 and 4) may have 0 to 4 correct answers. For each proposed answer, mark whether it is True or False, and provide a short justification (max 1 sentence). Marking for each question starts with full marks, and two marks are removed for each incorrect classification (each invalid answer selected, and each valid answer missed), down to a minimum of 0 marks.

Marking Scale. Partial marks will be given for answers that demonstrate general understanding but get details wrong (or forget them). In general (and where possible without fractional marks), getting 50% of the way to a full answer should net you roughly 70% of the marks. Effort beyond that will offer diminishing returns, so plan your work accordingly, and give yourself space and time to iterate on complex questions.

Q1 — Symmetric Cryptography — MAQs [30 marks]

Please recall the rules for marking MAQs stated in the preamble.

[6 marks] **1.a)** Alice and Bob share a 256 bit key known only to them. They have never used it in the past. Alice wants to encrypt and authenticate a single file to send to Bob. The file contains 2.4 Terabytes of recorded lecture material.

A. Alice can securely send the entire file by encrypting it using AES in ECB mode and computing a MAC over the ciphertext and nonce.

B. Alice can securely send the entire file in one message by encrypting it using AES in CTR mode, and computing a MAC over the ciphertext and nonce.

C. Alice can use the shared key as a One-Time Pad to encrypt the data, and as a MAC key to authenticate it.

D. Alice can use an integrated Authenticated Encryption algorithm, as long as it supports long messages.

[6 marks] **1.b)** Your friend Bozo designed a cool new blockcipher. It uses 128-bit keys, which are split into two 64-bit subkeys. For a (128-bit) key $k = (k_1, k_2)$ (where k_1 and k_2 are the subkeys) and a message m, the blockcipher computes its output as follows $\mathsf{Enc}_k(m) = \mathsf{Enc}'_{k_1}(\mathsf{Enc}'_{k_2}(m))$, where Enc′ is a blockcipher with 64-bit keys.

Assume that the best chosen plaintext attack against Enc′ recovers the key in 2^{64} encryptions.

A. A brute-force key recovery attack on Enc takes 2^{128} operations on average.

B. Enc is a lot more secure than Enc′.

C. The best attack on Enc takes 2^{128} operations.

D. The best attack on Enc takes 2^{65} operations.

+	□	▚	▞	■
□	□	▚	▞	■
▚	▚	□	■	▞
▞	▞	■	□	▚
■	■	▞	▚	□

Figure 1: Definition for the $+$ operator.

[6 marks] **1.c)** Consider the set $\mathcal{B} = \left\{\text{□}, \text{▚}, \text{▞}, \text{■}\right\}$ and the operator $+ \in \mathcal{B} \times \mathcal{B} \to \mathcal{B}$ defined by the table in Figure 1. Which of the following statements hold?

A. $\Pr\left[b \leftarrow\!\$\, \mathcal{B} : b \in \left\{\text{▚}, \text{▞}\right\}\right] = \frac{1}{2}$.

B. $\forall b \in \mathcal{B},\ b + b = \text{□}$.

C. $+$ with a fresh uniformly random key has perfect secrecy.

D. $\Pr\left[b_1 \leftarrow\!\$\, \mathcal{B}; b_2 \leftarrow\!\$\, \mathcal{B} : b_1 = b_2 = \text{▞}\right] = \frac{1}{4}$

Mary Poppins keeps lots of things in her handbag. She can summon objects out of her bag using the image of their name by some (possibly keyed) function f. The next two choices correspond to this scenario. e

[6 marks] **1.d)** Assume that f is a cryptographically secure pseudorandom function with 256-bit outputs, which Mary uses with a uniformly random key known only to herself. How many items can Mary store in her handbag before the probability that two items have the same tag becomes greater than $\frac{1}{2}$?

A. 2^{128}

B. 2^{256}

C. It depends on the length of the objects' names.

D. 2^{64}

[6 marks] **1.e)** Miss Poppins wants to use the mechanism for self-defence, and wants to hide from would-be muggers that she is summoning her pepper spray. She is particularly worried about repeat offenders hearing her summon her pepper spray once, and later recognizing the string she uses to summon it. Which of the following functions offer the right level of security in this scenario?

A. A collision-resistant hash function.

B. A secure nonce-based encryption scheme.

C. A secure IV-based encryption scheme.

D. A secure deterministic MAC.

Now you know where "supercalifragilisticexpialidocious" comes from, and you know to run when you hear it.

Q2 — Message Authentication Codes [10 marks]

2.a) We consider the security of MACs. Consider the following experiment, parameterized by a MAC scheme $\mathsf{M} = (\mathsf{Kg}, \mathsf{Tag}, \mathsf{Vfy})$.

```
$\mathsf{Exp}^{\mathsf{seuf\text{-}cma}}_{\mathsf{M}}(\mathbb{A})$
$K \leftarrow\$ \mathsf{Kg}$
$(\hat{M}, \hat{T}) \leftarrow\$ \mathbb{A}^{\mathcal{T}(\cdot)}$

    $\mathcal{T}(M)$
    $T \leftarrow \mathsf{Tag}_K(M)$
    return $T$
```

The *strong existential unforgeability under chosen message attack* advantage of some adversary $\mathbb{A}$ against some MAC scheme M is defined as follows, where a message-tag pair (M, T) is said to be fresh if the tag T was not produced for message M by the CMA oracle.

$$\mathsf{Adv}^{\mathsf{seuf\text{-}cma}}_{\mathsf{M}}(\mathbb{A}) = \Pr\left[\mathsf{Exp}^{\mathsf{seuf\text{-}cma}}_{\mathsf{M}}(\mathbb{A}) : \begin{array}{c}\mathsf{Vfy}_K\left(\hat{M}, \hat{T}\right) = \top \\ \wedge \left(\hat{M}, \hat{T}\right) \text{ is fresh}\end{array}\right]$$

[3 marks] i. Justify the adjective strong by proving that any sEUF-CMA secure MAC scheme is also EUF-CMA secure.

[2 marks] ii. Argue that the two notions are equivalent for deterministic MAC schemes.

2.b) Consider the following MAC scheme (simplified to take in a list of blocks, to avoid having to pad), constructed over a pseudorandom permutation E.

```
$\mathsf{Tag}_K(M[1] \| \ldots \| M[n])$
$X[1] \leftarrow K$
for $i$ in $\{2, \ldots, n+1\}$
    $X[i] \leftarrow E_{X[i-1]}(M[i-1])$
return $X[n+1]$
```

[3 marks] i. Show that the scheme is not EUF-CMA secure by describing a concrete forgery.

[2 marks] ii. Under what condition on the size of messages is the scheme UUF-CMA secure? Informally justify your answer. You can assume that E is a secure PRP.

Q3 — Security Notions for Digital Signatures [10 marks]

In this question, through some simple problems, we explore some of the security definitions for asymmetric cryptography, and how they relate to symmetric notions.

Syntax and Security of Signature Schemes A signature scheme is a triple of algorithms $\mathsf{S} = (\mathsf{Kg}, \mathsf{Sign}, \mathsf{Vfy})$, where Kg probabilistically produces a *key-pair* (split into a public key pk and a secret key sk), Sign probabilistically produces a *signature* given a secret key sk and a message m (we call this a signature on m under sk), and Vfy checks the validity of a signature given a public key, the signature and a message.

Consider the following experiments, parameterised by a signature scheme S and an adversary $\mathbb{A}$. In both cases, the adversary wins if the signature they output is both valid and fresh.

```
$\mathsf{Exp}^1_{\mathsf{S}}(\mathbb{A})$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow\$ \mathsf{Kg}$
$(\hat{m}, \hat{\sigma}) \leftarrow\$ \mathbb{A}^{\mathcal{S}(\cdot)}(\mathsf{pk})$

    $\mathcal{S}(m)$
    $\sigma \leftarrow\$ \mathsf{Sign}_{\mathsf{sk}}(m)$
    return $\sigma$
```

```
$\mathsf{Exp}^2_{\mathsf{S}}(\mathbb{A})$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow\$ \mathsf{Kg}$
$m^* \leftarrow\$ \mathcal{M}$
$\hat{\sigma} \leftarrow\$ \mathbb{A}^{\mathcal{S}(\cdot)}(\mathsf{pk})$

    $\mathcal{S}(m)$
    $\sigma \leftarrow\$ \mathsf{Sign}_{\mathsf{sk}}(m)$
    return $\sigma$
```

[1 mark] **3.a)** Why is the adversary given the public key as input? Justify this decision based on principles of modern cryptography.

[1 mark] **3.b)** Both experiments capture unforgeability notions. Which of Exp^1 and Exp^2 captures existential unforgeability? You may want to refer to similar symmetric notions for comparison.

[4 marks] **3.c)** Referring to similar notions of unforgeability for symmetric MACs, define advantages for both experiments. In particular, clarify the notion of validity and freshness.

[4 marks] **3.d)** Relate the two notions just defined by showing that one implies the other.

Q4 — Asymmetric Cryptography — MAQs [12 marks]

Please recall the rules for marking MAQs stated in the preamble.

[6 marks] **4.a)** Which of the following are valid key pairs? You may use a computer for this question, e.g. WolframAlpha will suffice (www.wolframalpha.com).

A. RSA secret key $(56, 154)$ with RSA public key $(13, 154)$.

B. Diffie-Hellman with group generator $g = 2 \pmod{59}$. Secret key 8 with public key 20. You may assume that 2 generates the whole group $\mathbb{Z}/59\mathbb{Z} - \{0\}$.

C. Diffie-Hellman with group generator $g = 2 \pmod{59}$. Secret key 9 with public key 21. You may assume that 2 generates the whole group $\mathbb{Z}/59\mathbb{Z} - \{0\}$.

D. RSA secret key $(5, 91)$ with RSA public key $(73, 91)$.

[6 marks] **4.b)** Which of the following statements are true:

A. For small parameters (e.g., computing discrete logarithms in a cyclic group of about 20 bits), on average, baby-step-giant-step and Pollard-rho will perform similarly.

B. For large parameters (e.g., computing discrete logarithms in a cyclic group of about 256 bits), on average, baby-step-giant-step and Pollard-rho will perform similarly.

C. Index calculus is the most efficient algorithm to solve the discrete logarithm problem in a group of size 2^{100}.

D. Index calculus can be used to solve the discrete logarithm problem in any group.

Q5 — Key-exchange and digital signatures [21 marks]

This question is about asymmetric primitives. Part (a) is about RSA, part (b) about ElGamal encryption, and part (c) is about ElGamal signatures.

[4 marks] **5.a)** You want to send an encrypted message to a friend with RSA public key $(e, n) = (13, 77)$. Using square-and-multiply, encrypt the message $m \equiv 3 \pmod{77}$ with their public key. You do not need a computer or calculator for this question but you may use one if you wish. Show your working.

5.b) Bob has sent you a message encrypted using ElGamal encryption with the integers mod $p = 103$. Your secret key is 59, Bob's public key is 94, your shared secret is 69, and the encrypted message is 86.

[5 marks] i. Using Euclid's algorithm to compute the inverse of the shared secret, decrypt the message. You do not need a computer or calculator for this question but you may use one if you wish. Show your working.

[5 marks] ii. You ask Bob to share the message with Alice, whose public key is $pk_A = 10$. You observe that Bob sends the ElGamal-encrypted message $(pk_B, \text{enc}_m) = (94, 70)$ to Alice. Encrypt the message $m = 4$ and send it to Bob as if you were Alice (using ElGamal encryption). You do not need a computer or calculator for this question but you may use one if you wish. Show your working.

[7 marks] **5.c)** You send messages $m_1 = 100 \pmod{226}$ and $m_2 = 11 \pmod{226}$ to your friend and they sign them using the ElGamal signature algorithm. They return the signed messages $(r_1, sig_1) = (171, 154)$ and $(r_2, sig_2) = (171, 3)$. Compute your friend's secret key. You do not need a computer or calculator for this question but you may use one if you wish. Show your working. You may use the following identities:

$$3 \cdot 151 = 226 \cdot 2 + 1$$

and

$$-112/171 \equiv 76 \pmod{226}.$$

Q6 — Cryptanalysis of the Discrete Logarithm Problem[17 marks]

[5 marks] **6.a)** i. Using Pollard-rho, find an integer a such that $3^a \equiv 14 \pmod{19}$. You do not need a computer or calculator for this question but you may use one if you wish. Show your working.

[4 marks] ii. Consider the following discrete logarithm problem of finding an integer b such that $14^b \equiv 13 \pmod{19}$. By applying index calculus on the factor base $\{2, 3\}$, we find the three equations

$$14^2 \equiv 2 \cdot 3 \pmod{19},$$

$$14^9 \equiv 2 \cdot 3^2 \pmod{19},$$

$$14^4 \cdot 13 \equiv 2^2 \cdot 3 \pmod{19}.$$

Use these to compute b. Show your working.

[2 marks] iii. Using your answers to parts (i) and (ii), calculate an integer c such that $3^c \equiv 13 \pmod{19}$.

[1 mark] iv. Does there exist an integer d such that $9^d \equiv 14 \pmod{19}$? Justify your answer.

[5 marks] **6.b)** Consider the finite field

$$\mathbb{F}_{3^2} = \{a + bx : a, b \in \mathbb{Z}/3\mathbb{Z}, x^2 + 2x + 2 \equiv 0 \pmod{3}\}.$$

The multiplicative group $\mathbb{F}_{3^2}^*$ has order 8 and is generated by $g = x$. Let $h = 2x + 2$. Using Pohlig-Hellman, compute an integer n such that $g^n = h$. You may use the following identities:

$$g^2 = x + 1, \qquad h^2 = 2.$$

UNIVERSITY OF BRISTOL

January 2023

Faculty of Engineering

Examination for the Degrees
of
Bachelor of Science
Master of Engineering
Master of Science

COMS30021(J)
Cryptology

TIME ALLOWED:
3 Hours

This paper contains 5 questions over 8 pages.
Answer all the questions.
The maximum for this paper is 100 marks.

Other Instructions

1. This is an open book exam.
2. Automated and programmable computing devices are permitted.

TURN OVER ONLY WHEN TOLD TO START WRITING

Preamble

This exam is composed of 5 questions, *all* of which you must answer. Questions are roughly ordered by increasing difficulty (as *we* perceive it). Within each question, question parts are roughly ordered by increasing difficulty (as *we* perceive it). Indicative difficulty is based on the complexity of the material, the depth of understanding required, *and* the level of guidance given. Some questions we mark as difficult may seem easy if you have engaged throughout. Conversely, some questions we mark as easy may seem difficult if you have not taken opportunities to practice the skills we teach or receive formative feedback.

Use of calculators and computers. You are free to use a computer or calculator throughout, but *must* show your working where specified. Wolfram Alpha[1] is sufficient for simple calculations. For more advanced questions, we expect you to use Sage or Python. In a bind, you can use Sage online via CoCalc.[2]

Open Book and Referencing. This is an open book exam conducted with access to an internet-connected computer. If you reference external material (material that we did not provide during the course of the unit), you *must* include clear references, in line with the University's academic integrity policy.

Marking MAQs. Multiple Answer Questions (Question 1) have between 0 and 4 correct answers. For each proposed answer, mark whether it is True or False, and provide a short justification (max 1 sentence). Marking for each question starts with full marks, and two marks are removed for each incorrect classification (each invalid answer selected, and each valid answer missed), down to a minimum of 0 marks.

Marking Scale. Partial marks will be given for answers that demonstrate general understanding but get details wrong (or forget them). In general (and where possible without fractional marks), getting 50% of the way to a full answer should net you roughly 70% of the marks. Effort beyond that will offer diminishing returns, so plan your work accordingly, and give yourself time and space to iterate on more complex questions.

[1] https://www.wolframalpha.com/

[2] https://cocalc.com/

Q1 — Multiple Answer Questions [30 marks]

[6 marks] **1.a)** (*) Alice and Bob roll one 6-sided die each.

A. Alice and Bob have probability $\frac{1}{6}$ of rolling the same value.

B. Alice and Bob have probability $\frac{1}{6}$ of both rolling a 1.

C. Alice and Bob have probability $\frac{1}{6}$ of rolling different values.

D. Alice has probability $\frac{1}{6}$ of rolling 1.

[6 marks] **1.b)** (*) Which of the following are valid RSA public keys (e, n)? You should use a computer for this question.

A. $(62, 5767)$

B. $(103, 1232)$

C. $(101, 2067)$

D. $(1073, 3233)$

[6 marks] **1.c)** (**) Alice and Bob share a 256-bit value k, known only to them, and generated uniformly at random. let E be a correct enciphering scheme that has perfect secrecy.

A. Without any further interaction, an adversary has probability 2^{-256} of recovering the value k.

B. An adversary who sees some message m and its enciphering $\mathsf{c} = \mathsf{E}_\mathsf{k}(\mathsf{m})$ has probability 2^{-256} of recovering the value k.

C. An adversary who sees some message m and its enciphering $\mathsf{c} = \mathsf{E}_\mathsf{k}(\mathsf{m})$ has probability 1 of recovering the value k.

D. Without any further interaction, an adversary has probability 1 of recovering the value k.

[6 marks] **1.d)** (**) Consider a cryptographic hash function with 256-bit digests. Which of the following hold?

A. The hash function is expected to have collision resistance, preimage resistance and second preimage resistance.

B. There exists a generic attack that computes the hash function q times and finds a collision with probability roughly $\frac{q}{2^{256}}$.

C. There exists a generic attack that computes the hash function q times and finds a collision with probability roughly $\frac{q^2}{2^{256}}$.

D. There exists a generic attack that computes the hash function q times and finds a preimage with probability roughly $\frac{q}{2^{256}}$.

[6 marks] **1.e)** (***) For which of the following values of p and $f(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$ is $(\mathbb{Z}/p\mathbb{Z})/(f(x))$ a finite field?

A. $(p, f) = (5, x^2 + 2)$
B. $(p, f) = (3, x^2 + 1)$
C. $(p, f) = (3, x^4 + 2x^2 + 1)$
D. $(p, f) = (2, x^2 + 1)$

```
$\mathsf{CBC.Enc}^{\mathsf{n}}_{\mathsf{k}}(\mathsf{m}[1]\|\ldots\|\mathsf{m}[b])$
$\mathsf{c}[0] \leftarrow \mathsf{n}$
for $i \in [1 \ldots b]$
    $\mathsf{c}[i] \leftarrow \mathsf{E}_{\mathsf{k}}(\mathsf{m}[i] \oplus \mathsf{c}[i-1])$
return $\mathsf{c}[1]\|\ldots\|\mathsf{c}[b]$
```

Figure 1: Encryption for CBC.

```
$\mathsf{C^*\text{-}MAC.Tag}_{(\mathsf{k}_1,\mathsf{k}_2)}(\mathsf{m}[1]\|\ldots\|\mathsf{m}[b])$
$\mathsf{c}[0] \leftarrow \mathsf{n}$
for $i \in [1 \ldots b]$
    $\mathsf{c}[i] \leftarrow \mathsf{E}_{\mathsf{k}_1}(\mathsf{m}[i] \oplus \mathsf{c}[i-1])$
return $\mathsf{E}_{\mathsf{k}_2}(\mathsf{c}[b])$
```

Figure 2: Tagging for C*-MAC.

```
$\mathsf{BadAE.Enc}^{\mathsf{n}}_{(\mathsf{k}_1,\mathsf{k}_2)}(\mathsf{m}[1]\|\ldots\|\mathsf{m}[b])$
$\mathsf{c}[0] \leftarrow \mathsf{n}$
for $i \in [1 \ldots b]$
    $\mathsf{c}[i] \leftarrow \mathsf{E}_{\mathsf{k}_1}(\mathsf{m}[i] \oplus \mathsf{c}[i-1])$
$\mathsf{t} \leftarrow \mathsf{E}_{\mathsf{k}_2}(\mathsf{c}[b])$
return $(\mathsf{c}[1]\|\ldots\|\mathsf{c}[b], \mathsf{t})$
```

Figure 3: Encryption for BadAE.

Q2 — Authenticated Encryption [20 marks]

This question explores the security of an integrated construction for authenticated encryption. We will consider only messages (including those generated by the adversary) whose length is a multiple of the block length.

Consider the construction BadAE shown in Figure 3, where E is a blockcipher with block length ℓ. Figure 1 recalls the encryption algorithm for the CBC mode of operation over the blockcipher E. Figure 2 recalls the tagging algorithm for the C*-MAC construction over the blockcipher E.

[2 marks] **2.a)** (*) Assume the key space for the blockcipher E is $\mathcal{K}$ (and the message space is $\{0,1\}^{\ell}$, as standard). What are the key space, message space, and ciphertext space for BadAE as an authenticated encryption scheme.

[4 marks] **2.b)** (*) Write the decryption algorithm for BadAE. Remember: check the tag.

[4 marks] **2.c)** (**) Express BadAE as a composition of CBC and C*-MAC. Which generic composition is it closest to? How does it differ from it?

[5 marks] **2.d)** (**) Describe a nonce-respecting adversary that produces a ciphertext that decrypts successfully to a message that was not queried to the encryption oracle. Your adversary may make a chosen-plaintext query before producing her forgery.

[5 marks] **2.e)** (***) Describe a nonce-respecting adversary against the IND-security of BadAE as a nonce-based encryption scheme. Your adversary may make two CPA queries.

Q3 — Key Exchange and Digital Signatures [20 marks]

This question is about ElGamal encryption and ElGamal signatures. You should use a computer for this question.

3.a) (*) You want to send an encrypted message to Alice using ElGamal encryption. Alice sends you her public key $(p, g, pk_A) = (31, 3, 15)$.

[1 mark] i. Using Sage, Python, or a program of your choice, generate a random secret key sk_B and a random message $m \in \{1, \ldots, p-1\}$ for yourself. (If you are unable to generate these randomly, just choose some $sk_B, m > 7$ to use for the rest of this question).

[3 marks] ii. Using square-and-multiply, compute your shared secret with Alice. You may do this on pen-and-paper or write a computer program. In either case, show your work (copy down code where relevant).

[3 marks] iii. Using double-and-add, compute your encrypted message. You may do this on pen-and-paper or write a computer program. In either case, show your work (copy down code where relevant).

[7 marks] **3.b)** (**) You ask Alice, who has public key $(p, g, pk_A) = (31, 3, 15)$, to sign two messages $m_1 = 12$ and $m_2 = 23$ using the ElGamal signature scheme. She sends you two signatures

$$(r_1, sig_1) = (24, 6) \text{ and } (r_2, sig_2) = (24, 23).$$

Find Alice's secret key. Show your working. You do not need a computer for this part but you may use one if you wish.
Hint: the possible multiples of $12 \pmod{30}$ are

$$\{12, -6, 6, -12, 0\}.$$

3.c) (***)

[2 marks] i. Let Alice's public key be as above in parts (a) and (b). Suppose that she sends you another signed message. If you wanted to recover, by brute-force, the nonce that she used, what is the maximum number of nonces that you have to check?

[2 marks] ii. How would you construct a (large) prime p to use in the setup for an ElGamal signature such that there are as little as possible valid choices for a valid nonce?

[2 marks] iii. Suppose p is specially constructed as in part (ii) and that g generates $\mathbb{F}_p^*$ as a multiplicative group. Is brute-force the best algorithm to find a nonce k given $r = g^k \pmod{p}$? Justify your answer.

Q4 — Cryptanalysis of the DLP [20 marks]

This question is about algorithms to solve the Discrete Logarithm Problem. You should use a computer for this question.

[4 marks] **4.a)** (*) Using index calculus with factor base $\{2, 3, 5\}$, find a such that $492^a \equiv 507 \pmod{569}$. You may use without proof that 492 is a generator of $\mathbb{F}_{569}^*$. Show your work (copy down code where relevant).

[8 marks] **4.b)** (***) Re-solve part (a) using Pohlig-Hellman, additionally making use of a square-root complexity algorithm to find discrete logarithms in the subgroup of $\mathbb{F}_{569}^*$ of order 71. Show your work (copy down code where relevant).

4.c) (***)

[2 marks] i. Comment on the concrete complexity of the algorithm you used for (a) versus the algorithm you used for (b).

[2 marks] ii. For 5 random choices of generator g for $\mathbb{F}_{569}^*$, by looking at factorizations of $g^i \pmod{569}$ for small i, comment on the ease of finding a suitable factor base.
If you are not sure how to compute generators, you can sacrifice one mark and instead look at 5 random numbers in $\mathbb{F}_{569}^*$.
Show your work (copy down code where relevant).

[2 marks] iii. How would you expect Pohlig-Hellman (including a square-root complexity subroutine) to perform with respect to index calculus in the computation of logarithms base g, where the g are those you found in part (ii)?

[2 marks] iv. Suppose that G is a cyclic group that is not the unit group of a finite field, and that the discrete logarithm problem is hard in G. Suppose further that G has 105663913 elements. How would you go about computing discrete logarithms in G? Justify your answer.

```
$\mathsf{Exp}^1(\mathbb{A})$
$\mathsf{a} \leftarrow_{\$} (\mathbb{Z}/p\mathbb{Z})^\times$
$\mathsf{b} \leftarrow_{\$} (\mathbb{Z}/p\mathbb{Z})^\times$
$\mathsf{r} \leftarrow_{\$} \mathbb{A}(g^{\mathsf{a}}, g^{\mathsf{b}})$
```

$$\mathsf{Adv}^1(\mathbb{A}) = \Pr\left[\mathsf{Exp}^1(\mathbb{A}) : \mathsf{r} = g^{\mathsf{a}\cdot\mathsf{b}}\right]$$

Figure 4: Experiment 1

```
$\mathsf{Exp}^2(\mathbb{A})$
$\mathsf{a} \leftarrow_{\$} (\mathbb{Z}/p\mathbb{Z})^\times$
$\mathsf{r} \leftarrow_{\$} \mathbb{A}(g^{\mathsf{a}})$
```

$$\mathsf{Adv}^2(\mathbb{A}) = \Pr\left[\mathsf{Exp}^2(\mathbb{A}) : \mathsf{r} = \mathsf{a}\right]$$

Figure 5: Experiment 2

```
$\mathsf{Exp}^{3\text{-real}}(\mathbb{A})$
$\mathsf{a} \leftarrow_{\$} (\mathbb{Z}/p\mathbb{Z})^\times$
$\mathsf{b} \leftarrow_{\$} (\mathbb{Z}/p\mathbb{Z})^\times$
$\mathsf{c} \leftarrow \mathsf{a}\cdot\mathsf{b}$
$\mathsf{r} \leftarrow_{\$} \mathbb{A}(g^{\mathsf{a}}, g^{\mathsf{b}}, g^{\mathsf{c}})$
```

```
$\mathsf{Exp}^{3\text{-ideal}}(\mathbb{A})$
$\mathsf{a} \leftarrow_{\$} (\mathbb{Z}/p\mathbb{Z})^\times$
$\mathsf{b} \leftarrow_{\$} (\mathbb{Z}/p\mathbb{Z})^\times$
$\mathsf{c} \leftarrow_{\$} (\mathbb{Z}/p\mathbb{Z})^\times$
$\mathsf{r} \leftarrow_{\$} \mathbb{A}(g^{\mathsf{a}}, g^{\mathsf{b}}, g^{\mathsf{c}})$
```

$$\mathsf{Adv}^3(\mathbb{A}) = \left|\Pr\left[\mathsf{Exp}^{3-\mathsf{real}}(\mathbb{A}) : \mathsf{r}\right] - \Pr\left[\mathsf{Exp}^{3-\mathsf{ideal}}(\mathbb{A}) : \mathsf{r}\right]\right|$$

Figure 6: Experiment 3

Q5 — Asymmetric Assumptions and Reductions [10 marks]

Let p be a prime, and g be a generator of $\mathbb{Z}/p\mathbb{Z}$. Consider the three experiments and associated advantages displayed in Figures 4, 5, and 6.

[2 marks] **5.a)** (**) Which of these experiments defines:

i. the Discrete Logarithm Problem in $\mathbb{Z}/p\mathbb{Z}$?

ii. an indistinguishability property?

[4 marks] **5.b)** (***) Order the three assumptions by descending order of hardness. For example, recall from Lectures 1 and 4 that Key Recovery is harder than One-Wayness, which is harder than Indistinguishability.

[4 marks] **5.c)** (***) Prove either one of the two hardness comparisons from Q5.b. Marks will be given for laying out the reduction logic, for writing down the reduction, and for analysing it.

THIS IS THE END OF THE EXAM

UNIVERSITY OF BRISTOL

January 2021

Faculty of Engineering

Examination for the Degrees
of
Bachelor of Engineering
Master of Engineering

COMS30021(J)
Cryptology

TIME ALLOWED:
2 Hours

This paper contains 6 questions over 11 pages.
Answer all the questions.
The maximum for this paper is 100 marks.

Other Instructions

1. This is an open book exam.
2. Automated and programmable computing devices are permitted.
3. After completion of this exam, you will have 15 minutes to upload your submission to Blackboard.

Preamble

This exam is composed of 6 questions, *all* of which you must answer:

- 2 regarding *symmetric cryptography*;

Question	Points
Symmetric Cryptography — MCQs	15
Hashing Passwords	20
Total:	35

- 1 at the interface between symmetric and asymmetric cryptography; and

Question	Points
Hybrid Constructions, Practical Cryptography	25
Total:	25

- 3 regarding *asymmetric cryptography*.

Question	Points
Asymmetric Cryptography — MCQs	6
Cryptography in Prime-Order Fields	12
Cryptography in Extension Fields	22
Total:	40

Use of calculators. You are free to use a computer or calculator throughout, but *must* show your working where specified. Wolfram Alpha[1]is sufficient for most of the questions in this exam (at least those that are made easier by having access to a calculator), but feel free to use other tools.

Open Book and Referencing. This is an open book exam conducted online. If you reference external material (material that we did not provide during the course of the unit), you *must* include clear references, in line with the University's academic integrity policy.

[1] `https://www.wolframalpha.com/`

Marking MCQs. Multiple Choice Questions (in Questions 1 and 4) may have 0 to 4 correct answers. For each question, marking starts with full marks, and a mark is removed for each incorrect classification (each invalid answer selected, and each valid answer missed), down to a minimum of 0 marks. If you believe none of the proposed answers are valid, you *must* indicate so with "None" or some other way of noting that you have seen the question and made the conscious choice of not marking any answers as valid.

Marking Scale. Partial marks will be given for answers that demonstrate general understanding but get details wrong (or forget them). In general (and where possible without fractional marks), getting 50% of the way to a full answer should net you roughly 70% of the marks. Effort beyond that will offer diminishing returns, so plan your work accordingly, and give yourself space and time to iterate on complex questions.

Q1 — Symmetric Cryptography — MCQs [15 marks]

Please recall the rules for marking MCQs stated in the preamble.

[3 marks] **1.a)** Alice and Bob share an AES key known only to them. They have never used it in the past. Alice wants to encrypt a single file to send to Bob. The file contains 2.4 Terabytes of Pokemon pictures.

A. Alice can securely send the entire file in one message using AES in CTR mode.

B. Alice can securely send the entire file using AES in ECB mode.

C. Using CTR mode does not require a nonce in this scenario, if Alice does not want to keep communicating with Bob.

D. The file is too large to send securely in a single message, regardless of which mode is used.

1.b) Your favourite encryption scheme Enc (which uses 128-bit keys) is broken! It now takes only 2^{50} encryptions, given a plaintext-ciphertext pair, to retrieve the key. The next two choices refer to this scenario.

[3 marks] i. The attack is

A. A key recovery attack.

B. A known ciphertext attack.

C. An exhaustive search.

D. A preimage attack.

[3 marks] ii. You generate two keys k_1 and k_2 and encrypt the password p to your hard drive as $c = \mathsf{Enc}_{k_2}(\mathsf{Enc}_{k_1}(p))$. Your cat walks across your keyboard and deletes both k_1 and k_2. Using the best known attack, how long (approximately) would it take to retrieve them given c, p, and access to a machine that can perform 2^{32} encryptions per second.

A. A day.

B. A week.

C. A year.

D. More than a century.

[3 marks] **1.c)** Santa keeps the naughty list in a database on a computer. The list is kept as a list of entries of the form (n, t), where n is a name, and t some additional tag. A known naughty elf has unrestricted access to the computer, and Santa believes he can use the tag t to prevent the elf from removing his name from the naughty list. How can Santa use t to prevent the naughty elf from removing his name from the database?

A. Compute t as an encryption of n with AES in CTR mode.

B. Compute t as a MAC tag for n, computed using CMAC.

C. Compute t as a digest of n, computed using SHA-256.

D. No purely cryptographic solution can be used.

[3 marks] **1.d)** Consider the set $\mathcal{B} = \Big\{$□, ▚, ▞, ■$\Big\}$ and the operator $+ \in \mathcal{B} \times \mathcal{B} \to \mathcal{B}$ defined by the table in Figure 1.

+	□	▚	▞	■
□	□	▚	▞	■
▚	▚	▞	■	□
▞	▞	■	□	▚
■	■	□	▚	▞

Figure 1: Definition for the + operator.

Zero or more of the following statements hold. Which?

A. $\Pr\Big[b \leftarrow\!\$\, \mathcal{B} : b \in \Big\{$▚, ▞$\Big\}\Big] = \frac{1}{2}$.

B. $\forall b \in \mathcal{B},\ b + b =$ □.

C. + with a fresh uniformly random key has perfect secrecy.

D. $\Pr\Big[b_1 \leftarrow\!\$\, \mathcal{B}; b_2 \leftarrow\!\$\, \mathcal{B} : b_1 = b_2 =$ ▞$\Big] = \frac{1}{4}$

Q2 — Hashing Passwords [20 marks]

This question explores the use of cryptography to protect passwords while at rest in server databases.

Consider the following system S, which is parameterized by a hash function H. When a user u registers with password p, S stores the tuple $(u, r, \mathsf{H}(p\|r))$ in its database, where r is some random *salt*. When an attempt is made to authenticate user u with a password p', S retrieves the tuple $(u, r, \mathsf{H}(p\|r))$, computes $\mathsf{H}(p'\|r)$, and successfully authenticates the user u is $\mathsf{H}(p\|r) = \mathsf{H}(p'\|r)$. The hash function H is assumed to produce uniformly sampled outputs given uniformly sampled inputs. Assume the adversary does not learn H until the start of the attack.

[2 marks] **2.a)** Assume the distribution user u draws their password p from is completely unknown to the adversary. Denote with ℓ the length of digests output by the hash function H and with n the length of p. What is the probability that the adversary successfully authenticates as user u in one attempt?

2.b) Assume now that the adversary has access to the complete database of tuples held by S. It contains entries for U users.

[2 marks] i. What is an upper-bound on the probability that the adversary authenticates as user u in one attempt?

[5 marks] ii. Assume the adversary has no knowledge of the distribution in which any of the users (not just u) sample their passwords. What can you say about the probability that the adversary authenticates as *any* user in one attempt? Consider, in particular, the effect of the random salt on the adversary's ability to search for multiple matches at once, and of the same salt being used for multiple users.

2.c) A better hash function H′ has been standardised and you want your users to benefit from it. You recompute the entire database for S, so that the tuples are now of the form $(u, r, \mathsf{H}'(\mathsf{H}(p\|r)))$.

[2 marks] i. Why would you not instead replace all entries in S's database with $(u, r, \mathsf{H}'(p\|r))$?

[2 marks] ii. Describe how authentication attempts (with a user u and a password p') are processed.

[7 marks] iii. Assume H is now broken (so that it is easy to compute preimages for any of its outputs). Show that the hash function $\mathsf{H}' \circ \mathsf{H}$ is preimage-resistant if H′ is preimage-resistant.

Q3 — Hybrid Constructions, Practical Cryptography[25 marks]

In this question, we consider constructions that combine symmetric and asymmetric cryptography. We focus on Key Encapsulation Mechanisms, and their use in constructing Hybrid Public Key Encryption.

In the rest of this question, we use a fixed cyclic group $\mathbb{G}$ of prime order q; we use g to denote some fixed generator of $\mathbb{G}$. In addition, we use a hash function H, which we will use as a Key Derivation Function; and a symmetric authenticated encryption scheme $\mathcal{E}$. All definitions below are specialised to this setting.

Key Encapsulation Mechanisms. A Key Encapsulation Mechanism (KEM) is a triple of algorithms $\mathcal{K} = (\mathsf{KGen}, \mathsf{Encap}, \mathsf{Decap})$, where:

KGen: probabilistically generates a keypair in $\mathbb{Z}_q \times \mathbb{G}$;

Encap: given a recipient's public key (in $\mathbb{G}$) and a sender's private key (in $\mathbb{Z}_q$), probabilistically generates a symmetric key (in some keyspace $\mathbb{K}$ and its encapsulation (in some set $\mathbb{E}$); and

Decap: given a recipient's secret key (in $\mathbb{G}$) and an encapsulation, recovers a symmetric key.

We do not use KGen in the following, but note for completeness that both schemes we define use standard Diffie-Hellman key generation in $\mathbb{G}$.

An KEM $\mathcal{K}$ is said to be correct if, for all $\mathsf{sk}_R, \mathsf{sk}_S \in \mathbb{Z}_q$, if $(\mathsf{k}, \mathsf{c}) \leftarrow\!\$\, \mathcal{K}.\mathsf{Encap}_{\mathsf{pk}_R}(\mathsf{sk}_S)$ then $\mathcal{K}.\mathsf{Decap}_{\mathsf{sk}_R}(\mathsf{c}) = \mathsf{k}$. (Where $\mathsf{pk}_R = g^{\mathsf{sk}_R}$.)

Figures 2 and 3 show two KEMs, which we study in more detail below. Note that AKEM_0 uses $\mathbb{E} = \mathbb{G}$, while AKEM_1 uses $\mathbb{E} = \mathbb{G} \times \mathbb{G}$.

```
AKEM_0

$\mathsf{Encap}_{\mathsf{pk}_R}(\mathsf{sk}_S)$
    $\mathsf{dh} \leftarrow \mathsf{pk}_R^{\mathsf{sk}_S}$
    $\mathsf{k} \leftarrow \mathsf{H}(\mathsf{dh}, \mathsf{pk}_R)$
    return $(\mathsf{k}, g^{\mathsf{sk}_S})$

$\mathsf{Decap}_{\mathsf{sk}_R}(\mathsf{pk}_S)$
    $\mathsf{dh} \leftarrow \mathsf{pk}_S^{\mathsf{sk}_R}$
    $\mathsf{k} \leftarrow \mathsf{H}(\mathsf{dh}, g^{\mathsf{sk}_R})$
    return $\mathsf{k}$
```

Figure 2: The AKEM_0 KEM.

```
AKEM_1

$\mathsf{Encap}_{\mathsf{pk}_R}(\mathsf{sk}_S)$
    $\mathsf{sk}_E \leftarrow\!\$\, \mathbb{Z}_q$
    $\mathsf{k} \leftarrow \mathsf{H}(\mathsf{pk}_R^{\mathsf{sk}_E} \| \mathsf{pk}_R^{\mathsf{sk}_S}, \mathsf{pk}_R)$
    return $(\mathsf{k}, (g^{\mathsf{sk}_E}, g^{\mathsf{sk}_S}))$

$\mathsf{Decap}_{\mathsf{sk}_R}(\mathsf{pk}_E, \mathsf{pk}_S)$
    $\mathsf{dh} \leftarrow \mathsf{pk}_E^{\mathsf{sk}_R} \| \mathsf{pk}_S^{\mathsf{sk}_R}$
    $\mathsf{k} \leftarrow \mathsf{H}(\mathsf{dh}, g^{\mathsf{sk}_R})$
    return $\mathsf{k}$
```

Figure 3: The AKEM_1 KEM.

Hybrid Public Key Encryption. KEMs can be used, in combination with a Data Encapsulation Mechanism (DEM), to implement Hybrid Encryption.

Here, we focus on the construction of Hybrid Public Key Encryption (HPKE) by simply using the key generated by the KEM in the Authenticated Encryption scheme $\mathcal{E}$, used as a DEM.

Given a DH keypair $(\mathsf{sk}_S, \mathsf{pk}_S)$ for the sender, a DH keypair $(\mathsf{sk}_R, \mathsf{pk}_R)$ for the recipient, some nonce n, and some message m, encryption in HPKE based on KEM $\mathcal{K}$ proceeds by:

1. using $\mathcal{K}$.Encap to generate a symmetric key k and its encapsulation e;
2. encrypting the message m with nonce n under key k with $\mathcal{E}$ into a ciphertext c; and
3. sending both c and e to the recipient.

This is described more formally in Figure 4.

```
$\mathsf{Enc}^{\mathsf{n}}_{\mathsf{sk}_S,\mathsf{pk}_R}(\mathsf{m})$
$(\mathsf{k}, \mathsf{e}) \leftarrow\!\$\ \mathcal{K}.\mathsf{Encap}_{\mathsf{pk}_R}(\mathsf{sk}_S)$
$\mathsf{c} \leftarrow\!\$\ \mathcal{E}.\mathsf{Enc}^{\mathsf{n}}_{\mathsf{k}}(\mathsf{m})$
return $(\mathsf{c}, \mathsf{e})$
```

Figure 4: Hybrid Public Key Encryption

[3 marks] **3.a)** Show that AKEM_1 is correct as a KEM.

3.b) We like decrypting things.

[3 marks] i. Describe the decryption algorithm $\mathsf{Dec}^{\mathsf{n}}_{\mathsf{pk}_S,\mathsf{sk}_R}(\mathsf{m})$ for HPKE.

[5 marks] ii. Give a reasonable definition of correctness for HPKE, and prove your decryption algorithm correct, assuming the correctness of the underlying KEM $\mathcal{K}$ and encryption scheme $\mathcal{E}$.

3.c) We now consider the property of Perfect Forward Secrecy. Consider a scenario where Alice (with keypair $(\mathsf{sk}_A, \mathsf{pk}_A)$) and Bob (with keypair $(\mathsf{sk}_B, \mathsf{pk}_B)$) have exchanged multiple ciphertexts encrypted using HPKE with AKEM_0, which Nadia has collected. Nadia nabs Bob off the street, and tickles him until he breaks and reveals sk_B.

[3 marks] i. Argue that Nadia can retrieve *all* plaintexts from the collected ciphertexts, including those sent by Bob to Alice.

[4 marks] ii. Argue (without proving) that Nadia would have been unable to retrieve *past* plaintexts from Bob to Alice had Alice and Bob used AKEM_1 instead.

3.d) We now study a couple of implementation considerations.

[2 marks] i. Give one example of a side-channel in this exam paper's text. (There is nothing in the binary, don't waste time there.) What does it tell you about the University of Bristol's Computer Science Department's exam preparation process, or about one of your examiners' hobbies?

[5 marks] ii. Consider an implementation of HPKE that uses a theoretically secure MAC-then-Encrypt construction as its DEM component, and a secure KEM. Describe the process through which decryption must occur for the implementation to be as secure as the specification. Give details of the ordering of operation and any implementation specific measures needed.

Q4 — Asymmetric Cryptography — MCQs [6 marks]

Please recall the rules for marking MCQs stated in the preamble.

[3 marks] **4.a)** Which of the following RSA key pairs are valid? You may use a computer for this question.

A. sk, pk $= (5, 187), (3, 187)$.
B. sk, pk $= (59, 4362), (781, 4362)$.
C. sk, pk $= (916, 10379), (357, 7031)$.
D. sk, pk $= (19, 77), (24, 77)$.

[3 marks] **4.b)** For which of the following choices of

$$f(x) = x^d + c_{d-1}x^{d-1} + \cdots + c_1 x + c_0$$

with $c_i \in \mathbb{Z}/2\mathbb{Z}$ does the set

$$\{a_{d-1}x^{d-1} + \cdots + a_0 : a_i \in \mathbb{Z}/2\mathbb{Z},\ f(x) \equiv 0\}$$

define a finite field?

A. $f(x) = x^2 + x + 1$.
B. $f(x) = x^3 + x^2 + x + 1$.
C. $f(x) = x^3 + x + 1$.
D. $f(x) = x^4 + 1$.

Q5 — Cryptography in Prime-Order Fields [12 marks]

You may use a computer for this question if you wish but you must show your working. Consider the finite field $\mathbb{F}_{101}$. The element $2 \in \mathbb{F}_{101}^*$ has order 100, so generates the group $\mathbb{F}_{101}^*$ (you do not have to show this).

[4 marks] **5.a)** Using the baby-step-giant-step algorithm, compute $a \pmod{100}$ such that $2^a \equiv 53 \pmod{101}$. You may use without proof that

$$2^{-10} \equiv 65 \pmod{101}.$$

[5 marks] **5.b)** i. Solving the same problem with Pollard-ρ yields a chain

$$(G_0, b_0, c_0) \ldots (G_{22}, b_{22}, c_{22})$$

(where, for each i, we have $G_i = 2^{b_i} \cdot (2^a)^{c_i}$), for which $G_{22} = G_6$ and $G_i \neq G_j$ for all $6, 22 \neq i \neq j$. Which method was more efficient in this instance? Justify your answer.

[3 marks] ii. How does the complexity of these examples compare to the asymptotic complexities of baby-step-giant-step and Pollard-ρ?

Q6 — Cryptography in Extension Fields [22 marks]

6.a) Consider the finite field

$$\mathbb{F}_{3^2} = \{a + bx : a, b \in \mathbb{Z}/3\mathbb{Z}, x^2 + 1 \equiv 0 \pmod 3\}.$$

[3 marks] i. By 'brute-force', find an integer n for which $(1+x)^n \equiv 2 + 2x$ in $\mathbb{F}_{3^2}$.

[5 marks] ii. Name one element that generates $\mathbb{F}_{3^2}^*$ and two elements that don't generate $\mathbb{F}_{3^2}^*$. Justify your answer.

[3 marks] iii. How many choices of generator are there for $\mathbb{F}_{3^2}^*$? Justify your answer.

[4 marks] **6.b)** Consider the finite field

$$\mathbb{F}_{3^3} = \{a + bx + cx^2 : a, b, c \in \mathbb{Z}/3\mathbb{Z}, x^3 + 2x + 1 \equiv 0 \pmod 3\}.$$

The multiplicative group $\mathbb{F}_{3^3}^*$ is generated by $g = x + 1$ (you do not have to show this). We will use this setup for a Diffie-Hellman key exchange: your secret key is $\mathsf{sk}_D = 5$, and Hellman's public key is $x^2 + 2 = \mathsf{pk}_H = g^{\mathsf{sk}_H}$. Using the square-and-multiply algorithm, compute your and Hellman's shared secret key.

6.c) You should use a computer for this question. Wolfram Alpha is sufficient for what you need to do, but use any programme of your choice. Do not submit any code.

[5 marks] i. Which *two* algorithms to compute discrete logarithms would be most efficient for the finite field $\mathbb{F}_{3^{54}}$? Justify your answer.

[2 marks] ii. Are the algorithms you gave more or less efficient for solving discrete logarithms in $\mathbb{F}_{3^{53}}$? Justify your answer.