Calculators may be used in this examination provided they are not capable of being used to store alphabetical information other than hexadecimal numbers

UNIVERSITY OF BIRMINGHAM

School of Computer Science

Network Security and Cryptography

Main Summer Examinations 2024

Time allowed: 2 hours

[Answer all questions]

Note

Answer ALL questions. Each question will be marked out of 20. The paper will be marked out of 48, which will be rescaled to a mark out of 100.

Question 1 Symmetric-Key Cryptography

Consider the following hash function H:

> **INPUT:** a bitstring x of length less than 2^{64}
> Let $y = \text{SHA256}(x)$
> Let $z =$ the first 60 bits of y
> **OUTPUT:** z

(a) How many bits does H output? **[5 marks]**

Fred wants to find a collision for H. He runs the following program (note: "bin" is a function that converts an integer to the binary representation of the integer. For example, bin(12) is '1100'):

```
Let x = H(bin(0))
Let y = 1
Let z = H(bin(y))
while x ≠ z:
    Let y = y + 1
    Let z = H(bin(y))
print('Collision found:', bin(0), 'and', bin(y))
```

(b) Approximately how many iterations of the loop do you expect this program to take? **[5 marks]**

(c) Write pseudocode for a program that finds a collision for H. Your program should take about 2^{30} iterations of its main loop. **[5 marks]**

(d) Briefly describe the memory requirements for your program. **[5 marks]**

Question 2 Public-Key Cryptography

(a) Suppose you are given a Public-Key encryption scheme which is IND-CPA secure. Justify why the scheme achieves One-Way security. **[5 marks]**

(b) Consider the following modification of ElGamal encryption where two messages, encoded as two numbers between 2 to $p-2$, are encrypted simultaneously.

Procedure $\mathsf{Keygen}(1^\lambda)$	Procedure $\mathsf{Encrypt}(PK, m_1, m_2)$
01 : Choose a 2048 -bit prime p and a number $g < p$	// Note, both $m_1, m_2 \in \{2, \ldots, p-2\}$
02 : $x \xleftarrow{\$} \{1, \ldots, p-1\}$	01 : Parse $PK = g, X$
03 : $SK = x, PK = (g, g^x \bmod p)$	02 : $y \xleftarrow{\$} \{2, \ldots, p-2\}$
04 : **return** SK, PK	03 : $c_1 = g^y \bmod p$
	04 : $c_2 = m_1 \cdot X^y \bmod p$
	05 : $c_3 = m_2 \cdot X^{2y} \bmod p$
	06 : **return** $c = (c_1, c_2, c_3)$

(i) Write the decryption algorithm and derive its correctness. **[3+2 marks]**

(ii) Justify why this scheme is One-Way secure. **[5 marks]**

(iii) Show that the scheme is not IND-CPA secure. **[5 marks]**

Question 3 Network security

(a) For each of the following statements, consider whether it is true or false and write down the answer for each statement in your answer book. Justify each answer in at most 1–2 sentences.

(i) It is easier to detect an active attacker than a passive attacker.

(ii) HeartBleed was an error in a key exchange protocol.

(iii) WPA2 provides forward secrecy.

(iv) TLS downgrading attacks require both parties to support weak ciphers.

(v) VPNs provide similar anonymity guarantees as Tor.

(vi) iMessage requires its users to trust Apple.

[6 marks]

(b) Consider the following weakened version of the station-to-station protocol:

1: $A \rightarrow B : g^x$
2: $B \rightarrow A : g^y, S_B(g^x)$
3: $A \rightarrow B : \{S_A(g^x, g^y)\}_{g^{xy}}$
4: $B \rightarrow A : \{M\}_{g^{xy}}$

where:

- $\{X\}_k$ denotes symmetric encryption of X using key k
- $S_Y(X)$ denotes the asymmetric signature of X, constructed using Y's private key
- The public keys of A and B are globally known
- All exponentiation operations are performed over a prime modulus p
- g and p are globally known, x is chosen by A and y is chosen by B
- M is the message to be transmitted
- x, y, g^{xy} are not stored after the protocol run

(i) Considering a passive attacker, does this protocol provide confidentiality, data integrity, authentication, and forward secrecy? Briefly explain your answer.

[4 marks]

(ii) Considering an active attacker, can you craft an attack where the attacker C impersonates B (i.e., in message 4, A believes that B sent the message M, although actually M is controlled by the attacker C)? Use the same notation as above. Briefly explain why this attack is possible.

[6 marks]

End of Paper

(iii) Can you provide a fix for the protocol?

[4 marks]

Do not complete the attendance slip, fill in the front of the answer book or turn over the question paper until you are told to do so

Important Reminders

- Coats/outwear should be placed in the designated area.
- Unauthorised materials (e.g. notes or Tippex) must be placed in the designated area.
- Check that you do not have any unauthorised materials with you (e.g. in your pockets, pencil case).
- Mobile phones and smart watches **must** be switched off and placed in the designated area or under your desk. They must not be left on your person or in your pockets.
- You are not permitted to use a mobile phone as a clock. If you have difficulty seeing a clock, please alert an Invigilator.
- You are not permitted to have writing on your hand, arm or other body part.
- Check that you do not have writing on your hand, arm or other body part – if you do, you must inform an Invigilator immediately
- Alert an Invigilator immediately if you find any unauthorised item upon you during the examination.

Any students found with non-permitted items upon their person during the examination, or who fail to comply with Examination rules may be subject to Student Conduct procedures.