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

LM Network Security and Cryptography

Main Summer Examinations 2023

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 60, which will be rescaled to a mark out of 100.

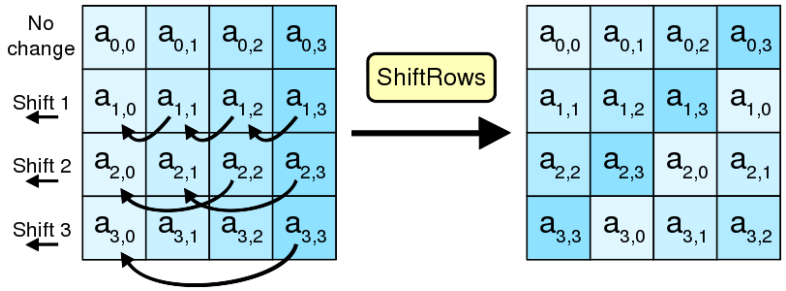
Question 1 (Symmetric-key cryptography)

Let message M and key K be the following 16 byte values:

$$M = \texttt{0x01020304 01020304 01020304 01020304}$$
$$K = \texttt{0x0F0F0F0F 0F0F0F0F 0F0F0F0F 0F0F0F0F}$$

Recall that, in AES, the first round key K_0 is equal to the principal key K. The first three steps of running AES with K on M consist of (i) XOR with the first round key; (ii) running SubBytes; and (iii) running ShiftRows. The SubBytes table and an illustration of the ShiftRows operation are shown below.

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
00	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
30	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
40	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16



(a) What is the result of each of the three steps (i), (ii), (iii), run in turn? **[6 marks]**

(b) Suppose parties A and B have established a shared key K. Consider the following scheme to send a message m from A to B:

- A computes $K_1 = \text{kdf}(K, 1)$ and $K_2 = \text{kdf}(K, 2)$.
- A computes $X = \text{Enc}(K_1, m)$ and $Y = \text{HMAC}(K_2, m)$ and sends them to B.
- B computes K_1 and K_2 in the same way as A, and receives X and Y.
- B computes $m' = \text{Dec}(K_1, X)$ and $Y' = \text{HMAC}(K_2, m')$.
- B checks that $Y = Y'$ and, if so, considers that m' is the message that A sent.

(i) If both parties behave correctly, is the scheme correct in the sense that $m = m'$? Explain your answer.

(ii) Does the scheme satisfy IND-CPA? Explain your answer.

[7 marks]

(c) A start-up company has implemented an end-to-end encrypted messaging app. Suppose there is already a conversation thread between two users A and B, and they have already established a shared key K. The message sending-and-receiving part of the app works as follows:

- If A wants to send a message M to B, then A's app prepares the encryption $\text{Enc}_K(M)$ and sends it to the company's server. Here, Enc is a good authenticated encryption scheme, such as AES in CTR mode and encrypt-then-MAC using HMAC-SHA2.
- The company's server then sends the encrypted message to B's app.
- B's app checks the authenticity of the message, and if that check is valid, it decrypts the message and displays it to B.

This solution is supposed to ensure that the confidentiality and integrity of the messages are preserved, even if the company's server is under the control of an attacker. Can an attacker change the *contents* of a message sent from A to B? Can an attacker change the *ordering* of two messages sent from A to B? Explain your answer. **[7 marks]**

Question 2 Public-key cryptography

Consider the following RSA based encryption scheme that we will call *NoHashPKC*.

Procedure $\mathsf{Keygen}(1^\lambda)$

01 : Choose two random $\lambda/2$-bit primes p and q
02 : $n = p \cdot q$
03 : $\phi = (p-1)(q-1)$
04 : Select e such that
$1 < e < \phi$ and $\gcd(e, \phi) = 1$
05 : Compute d such that
$1 < d < \phi$ and $ed \equiv 1 \pmod{\phi}$
06 : Set $PK = (e, n)$
07 : Set $SK = (d)$
08 : **return** (PK, SK)

Procedure $\mathsf{Encrypt}(PK, m)$

// We assume $m \in \mathbb{Z}_n^*$
01 : $r \xleftarrow{\$} \mathbb{Z}_n^*$
02 : $c_1 = r^e \bmod n$
03 : $c_2 = m \cdot r$
04 : **return** $c = (c_1, c_2)$

Procedure $\mathsf{Decrypt}(SK, c)$

01 : Parse $c = c_1, c_2$
02 : $m = c_2 \cdot c_1^{-d} \bmod n$
03 : **return** m

(a) Show that the NoHashPKC Algorithm is correct. **[5 marks]**

(b) Is the NoHashPKC Algorithm one-way? **[5 marks]**

(c) Show that the NoHashPKC scheme is *not* IND-CPA secure. **[10 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) AES-256 in CTR mode provides confidentiality and integrity.

(ii) Both key exchange and the encryption scheme are important to determine whether a protocol provides forward secrecy.

(iii) WEP uses the same encryption key for all connected devices.

(iv) Tor provides confidentiality when accessing webpages that are not secured via HTTPS.

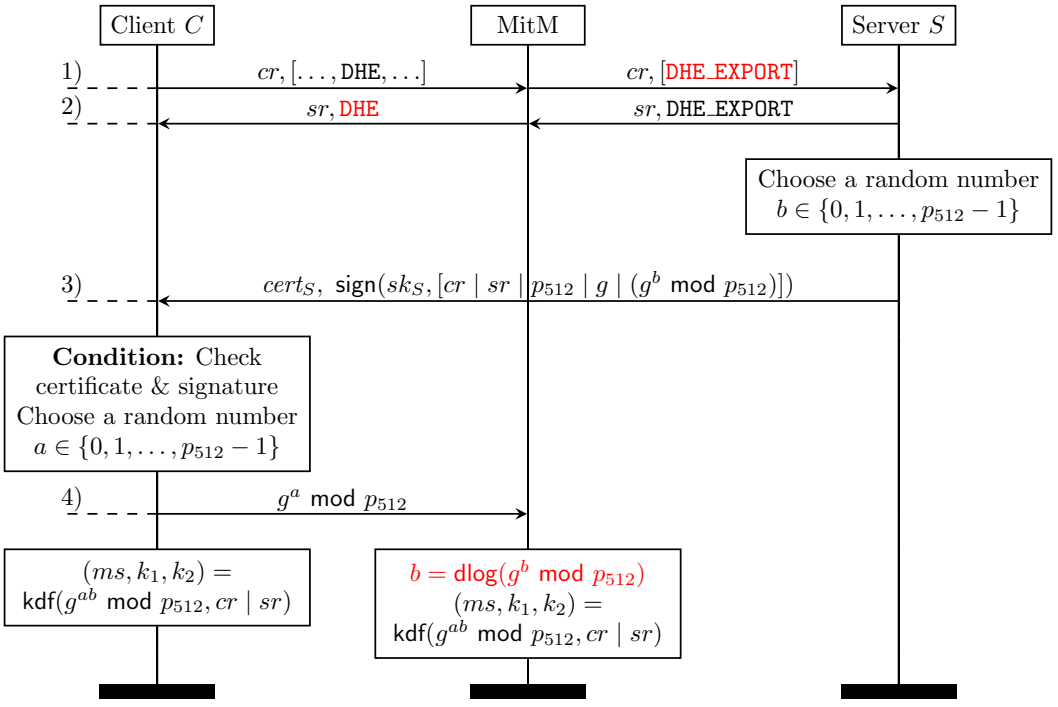
(v) DNSSEC provides authentication and data integrity, but not confidentiality.

(vi) `STARTTLS` provides end-to-end encryption for emails.

[3 marks]

(b) Recall the LogJam attack, which downgrades the cipher to an insecure version of Diffie-Hellman even if only the server supports that version. Below is an abbreviated attack diagram.

Logjam Attack Diagram



Note: cr and sr are the client's and server's respective nonces. $cert_S$ is the server's certificate and sk_S is the private key corresponding to the public key inside the certificate. g and p_{512} are the Diffie-Hellman parameters for `DHE_EXPORT`. kdf is a key derivation function that generates the keys used in the subsequent exchange of messages.

(i) Name two possible defenses against the LogJam attack (one for the client and server, respectively). Neither of these defenses should modify any messages exchanged between the parties. Explain how these defenses work. **[4 marks]**

(ii) Create a new defense against the LogJam attack **and** general ciphersuite downgrading attacks by modifying the simplified TLS protocol from the diagram above. In particular, your defense can

- modify message 3),
- modify the client-side check following message 3).

Explain how and why your defense works. Explain how your approach can defend against the LogJam attack and against ciphersuite downgrade attacks. **[8 marks]**

(iii) Suppose you managed to run a LogJam attack on a TLS exchange and observe:

$$\begin{aligned} p_{512} &= 17 \\ g &= 3 \\ (g^b \bmod p_{512}) &= 10 \\ (g^a \bmod p_{512}) &= 5 \end{aligned}$$

From this information, recover the secrets a, b, and $(g^{ab} \bmod p_{512})$. Show your workings. **[5 marks]**

End of Paper

This page intentionally left blank.

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.