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

Security and Networks

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

Question 1

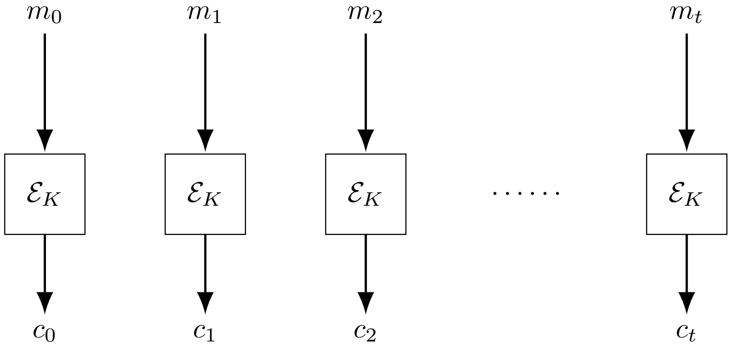
(a) Consider the following encoding of the English alphabet.

0	1	2	3	4	5	6	7	8	9	10	11	12
a	b	c	d	e	f	g	h	i	j	k	l	m

13	14	15	16	17	18	19	20	21	22	23	24	25
n	o	p	q	r	s	t	u	v	w	x	y	z

You received the ciphertext "czsdlbbus" that was generated by the one-time pad encryption scheme with the key "computing". Derive the plaintext. **[5 marks]**

(b) The block-cipher modes of operation are algorithms to encrypt long messages using block ciphers. In case of ECB mode, the message is divided into blocks, and each block is encrypted separately using the block cipher.



Explain why ECB is not used in practice. **[5 marks]**

(c) Google Trust Certifying Authority uses RSA hash and sign signature scheme. The RSA modulus *N* is 2048-bit and the *e* is set to be 65537. The following is the key-generation algorithm of RSA-2048

```
Procedure Keygen($1^\lambda$)
Choose two random 1024-bit primes $p$ and $q$
$N = p \cdot q$
$\phi = (p-1)(q-1)$
Select $e$ such that
    $1 < e < \phi$ and $\gcd(e, \phi) = 1$
Compute $d$ such that
    $1 < d < \phi$ and $ed \equiv 1 \pmod{\phi}$
Set $PK = (e, N)$
Set $SK = (d, N)$
return $(PK, SK)$
```

Explain why the corresponding RSA secret key d can never be an even number. **[5 marks]**

(d) Consider the following construction of a message authentication code (MAC) that takes a 256-bit key K and a 256-bit IV, and a binary string message M

$$\text{MAC}(IV, K, M) = (IV, \text{AES-Encrypt}_{IV}(H(M) \oplus K))$$

where H is the SHA-256 hash function and AES-Encrypt_{IV} is the AES encryption algorithm with IV used as the secret key. Justify why the construction is not a secure message authentication code. **[5 marks]**

Question 2

(a) Browsers allow access to cookies only if the domain of the cookie is the same as the domain for the website. Describe an attack which is prevented by this restriction. **[5 marks]**

(b) A website uses https for authentication but the link to the general conditions of use on the domain uses only http. How could an attacker get access to this website without authentication? **[5 marks]**

(c) Consider the following protocol:

$$\begin{array}{lcl} A & \rightarrow & B : E_{pk(B)}(N_A), A \\ B & \rightarrow & A : E_{pk(A)}(N_A, N_B, B) \\ A & \rightarrow & B : E_{pk(B)}(N_B) \\ A & \rightarrow & B : \{M\}_{\#(N_A, N_B)} \end{array}$$

where N_A and N_B are nonces, and $\#(N_A, N_B)$ is a symmetric key based on the hash of N_A and N_B, and $pk(A)$ is the public key of A. Is it possible for the attacker to learn M without knowing any of the private keys of A and B? If so, give an attack in Alice-Bob Notation. If not, explain why. **[10 marks]**

Question 3

You review the following C program that checks if you correctly guessed a random number. The function atoi tries to parse an integer number from a string and ignores any characters following the number. For example, atoi("12a3") == 12.

```
1  #include <stdio.h>
2  #include <string.h>
3
4  int main() {
5      int guess = 0;
6      int target = random();
7      char buffer[15];
8
9      printf("What's the random number?\n");
10     gets(buffer);
11
12     guess = atoi(buffer);
13
14     if(guess == target) {
15         printf("Admin access granted!\n");
16     } else {
17         printf("Password is wrong, sorry!\n");
18     }
19
20     return 0;
21 }
```

(a) Assume that the program is compiled for x86 in 32-bit mode and local variables are pushed onto the stack in the order specified in the program.

(i) Sketch the state of the stack *before* line 10 is executed. Clearly indicate where top and bottom of the stack are located. Assume that all variables are aligned at 1-byte boundaries.

(ii) Assume that random() returns the value 12. Sketch the state of the stack *after* line 12 has been executed. Where you can, indicate the values on the stack at this point for the following input: "15 is a number" (without the quotes)

[8 marks]

(b) Assume you want to gain admin access (i.e., execute line 15).

(i) Explain which vulnerability is present in this code.

(ii) Explain how you would craft an input to make the value of `target` be `0x212121` (hexadecimal representation). Note that the ASCII character `!` is represented as `0x21` in memory. If possible, give a concrete input.

(iii) Explain how you would craft an input to the function to exploit this vulnerability and reach line 15. If possible, give a concrete input.

[10 marks]

(c) Describe a way to fix the vulnerability in this code and explain why it is successful. **[2 marks]**

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.