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 2023

Time allowed: 2 hours

[Answer all questions]

Turn Over

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	13	14	15	16	17	18	19	20	21	22	23	24	25
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z

Derive the ciphertext generated by the one-time pad encryption scheme when the message M is "university" and the key K is "birmingham"

[6 marks]

(b) Suppose Alice is sending messages using textbook RSA encryption with public key $PK = (e, N)$. The corresponding private key $SK = (d, N)$ is only known to the receiver. The adversary got hold of a ciphertext c which is the encryption of some $m \in \mathbb{Z}_N^*$, unknown to the adversary.

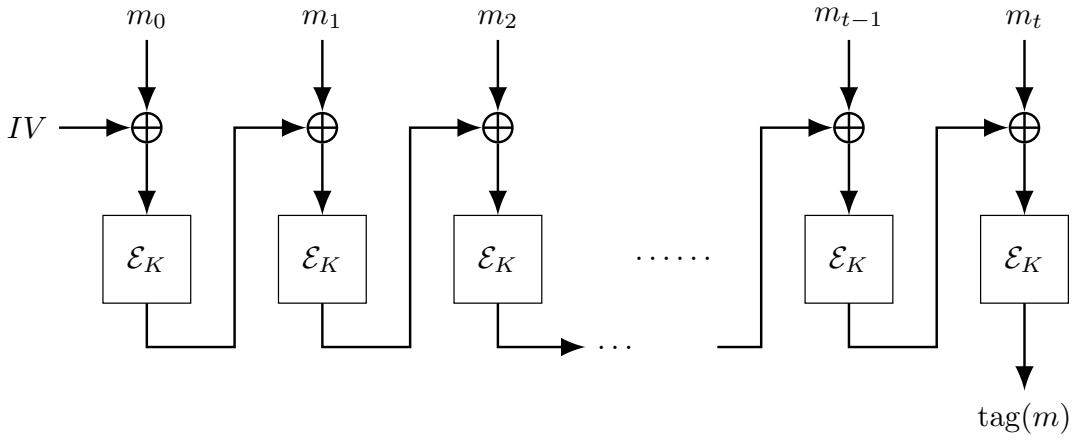
(i) How can the adversary create a ciphertext that would decrypt to $2m$ when decrypted using the corresponding secret key?

(ii) Justify why this ciphertext decrypts to $2m$ when decrypted using the corresponding secret key.

Remember, the adversary cannot decrypt c as the adversary does not know the secret key SK.

[7 marks]

(c) Consider the following modification of CBC-MAC. Note the IV is an all 0-bit string.



The modified version differs from the standard design in a crucial aspect. There is no length padding at the end. Show that the modification leads to an insecure mac. The adversary requests for MACs of some messages of their choice, and outputs a forgery (new message-MAC pair). Recall, the forgery must be on a message for which the adversary has not requested a MAC.

[7 marks]

Question 2

(a) Suppose you accept all certificates for a TLS-connection. Is this secure? If yes, explain why. If not, describe an attack. **[6 marks]**

(b) Suppose a webserver allows only cryptographic protocols that satisfy forward secrecy. Suppose the webserver forwards all encrypted traffic to a specific server with the intention that this server checks all traffic for malware. Is this possible if this server has access to the private key of the webserver? If yes, give a justification. If not, explain why and suggest changes to achieve this aim. **[7 marks]**

(c) Suppose each form in a website has a unique identifier which is the same for all requests. The webserver tries to prevent cross-site request forgery (CSRF) attacks as follows: When the webserver sends a form, it also sets a cookie consisting of the unique identifier of this form and a hidden form field which contains the MAC (Message authentication code) of this identifier with a key known only to the webserver. When the form is received, the webserver checks that the value of the hidden field is the MAC of the cookie. Does this scheme prevent CSRF attacks? If yes, give a justification. If not, explain why and suggest a modification which achieves this aim. **[7 marks]**

Question 3

You review the following C program that performs a password check:

```
1  int check_authentication(char *password) {
2      int authenticated = 0; // 0: not authenticated, else authenticated
3      char canary = 'a';
4      char password_buffer[16];
5
6      strcpy(password_buffer, password);
7      if(canary != 'a')
8          return 0;
9
10     if(strcmp(password_buffer, "mahgnimrib") == 0)
11         authenticated = 1;
12
13     return authenticated;
14 }
```

(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 6 is executed. Clearly indicate where top and bottom of the stack are located. Assume that all variables are aligned at 1-byte boundaries.

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

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

[7 marks]

(b) The author of the code intended to prevent this type of vulnerability using a self-made stack canary.

(i) Explain how a stack canary works and what types of attacks it can prevent.

(ii) Explain why this self-made stack canary is ineffective.

(iii) Is there a way of preventing the vulnerability from (a) by changing only the value of `canary`?

[7 marks]

(c) Mention two more protection mechanisms, which are typically used to prevent this kind of vulnerability. For each of those, elaborate whether they are successful in preventing your specific attack in (a). **[6 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.