UNIVERSITY OF BIRMINGHAM

School of Computer Science

Network Security and Cryptography

Main Summer Examinations 2021

Network Security and Cryptography

Question 1 (Symmetric-key cryptography)

A bank app and the bank server share a key K. When the user requests a transfer of \$1000.00 to account 12345678, the app uses AES128 in CTR mode to encrypt using the key K the message

`TRANS "1000.00" TO "12345678"`

(a) The message consists of 29 bytes. After encryption by AES128 in CTR mode, how many bytes are there in the ciphertext? (Don't forget to include the block for the nonce and the counter.) **[3 marks]**

Suppose the attacker can intercept and modify this message ciphertext as it travels from the app to the server.

(b) Explain how the attacker can modify the ciphertext so that when it is decrypted by the server, it will say

`TRANS "9999.99" TO "12345678".`

Your explanation should mention explicitly which bytes of the ciphertext the attacker will modify. **[4 marks]**

To avoid this attack, the bank programmer decides to use a MAC function to authenticate the message. Her design is as follows:

- From the key K, the app and the server derive two keys, $K_1 = \text{HMAC}_K(1)$ (to be used for encryption) and $K_2 = \text{HMAC}_K(2)$ (to be used for MAC).
- Send the encryption by AES128 in CTR mode using the key K_1 of the message `TRANS "1000.00" TO "12345678"`, together with the HMAC using key K_2 of the plaintext message `TRANS "1000.00" TO "12345678"`. When the server receives the message, it decrypts the first part with K_1, applies HMAC with K_2 to the result, and checks that this value equals the received HMAC. It rejects the message if the check fails.

(c) Is this method secure against the integrity attack of part (ii)? Explain your answer. **[5 marks]**

(d) Is this method secure against confidentiality attacks? Explain your answer. **[3 marks]**

Question 2 (Public-key cryptography)

Consider MElGamal, a variant of the ElGamal public key encryption (PKE) scheme, with encryption algorithm that only accepts plaintexts in $\{0,1\}$. MElGamal is defined as follows:

- Key generation (λ)
  - Let q, p be primes w.r.t. security parameter λ such that $q|p-1$
  - Let $g \neq 1$ be such that $g^q = 1 \mod p$
  - Let $\mathbf{G}$ be the subgroup of $\mathbf{Z}_p^\star$ generated by g
  - Let $x \overset{R}{\leftarrow} \mathbf{Z}_q$. Let $h = g^x \mod p$
  - Public-key : $PK = (p, q, g, h)$. Private-key : $SK = x$
- Encryption $(PK, m \in \{0,1\})$
  - m must be a single bit (i.e. $m \in \{0,1\}$).
  - Let $r \overset{R}{\leftarrow} \mathbf{Z}_q$
  - Output $c = (g^r \mod p,\ h^r \cdot g^m \mod p)$
- Decryption $(SK, C = (c_1, c_2))$
  - ...

(a) Define the decryption algorithm of MElGamal. Show that MElGamal satisfies the completeness property for PKE schemes. **[4 marks]**

(b) Is MElGamal an IND-CPA secure scheme? Justify your answer. **[3 marks]**

(c) Let us define an operation $\otimes$ over MElGamal ciphertext as follows: $(c_1, c_2) \otimes (c_1', c_2') := (c_1 \cdot c_2 \mod p,\ c_1' \cdot c_2' \mod p)$. Show that for any $m, m' \in \{0,1\}$ such that $m \neq m'$ holds that $\mathsf{Enc}(PK, m) \otimes \mathsf{Enc}(PK, m') = \mathsf{Enc}(PK, m \oplus m')$, where $\oplus$ is the XOR operation. **[5 marks]**

(d) Is MElGamal non-malleable? Justify your answer. **[3 marks]**

Question 3 (Network security)

Wireless networks are increasingly common, and in many organisations have almost completely replaced wired networks for client-device access.

(a) Explain the difference between WPA2 PSK (pre-shared key, also called WPA2 Personal) and WPA2 Enterprise. What criteria should one use to inform the choice between these two systems? Why might some companies be tempted to use WPA2 PSK instead of WPA2 Enterprise? **[9 marks]**

You are the network manager of a large shared office building which has many tenants from different organisations, all using a single shared wireless network secured with WPA2 PSK. You have been approached by one of the tenant organisations, who has concerns about the security of the wireless network, given the fact that everyone is using the same pre-shared key. They have asked you the following questions:

Q1 Can other tenants within the building read the emails that we send and receive?

Q2 Can other tenants send emails that look like they come from our organisation?

Q3 Can other tenants see what URLs we visit when web browsing? What about the content of the web pages?

Q4 Can other tenants access the shared drive we have in the building (it is meant to be accessible only to members of our organisation).

(b) Answer the questions as best you can. Mention any clarifications you would need to obtain, in order to give more precise answers. **[6 marks]**

The tenant organisation that approached you suggests you should upgrade the whole network to WPA2 Enterprise. You have been asked to respond to the CEO of the tenant organisation, advising her of the best course of action.

(c) Write a memo, of approximately half a page, briefing her on the issues. You should consider:

- What are the problems that using a single shared-key network for multiple enterprises will cause?
- What will need to be done to deploy WPA2 enterprise, and what will the costs be?
- What will be the benefits?
- Someone has suggested having both WPA2 PSK and WPA2 Enterprise at the same time. Could that work?

[15 marks]