UNIVERSITY OF BIRMINGHAM

School of Computer Science

Security and Networks First Class Test

Class Test 2020/21

Security and Networks First Class Test

Question 1

(a) Consider ElGamal encryption with $g = 7$, $p = 11$.

- Bob chooses $x = 4$ as the private key. What is his public key? Show your workings.
- What is the encryption of the message $m = 4$ with Bob's public key when choosing $r_A = 3$ as the random? Show your workings.

[10 marks]

(b) A client established the connection with the server as follows:

- Client and server agree on g and p as used in the Diffie-Hellman protocol.
- The client creates a random number x and sends $g^x \mathit{mod}\, p$ to the server.
- The server creates a random number y and sends $g^y \mathit{mod}\, p$ to the client.
- Every message between client and server is encrypted with AES in counter mode using the $g^{xy} \mathit{mod}\, p$ as the key. In addition the SHA256 hash of each message is sent as well.

(i) Is $g^{xy} \mathit{mod}\, p$ a good key for client and server? If this is the case, provide a justification. If not, explain why.

(ii) Does this protocol provide authenticated encryption? If this is the case, provide a justification. If not, explain why and provide a remedy. **[10 marks]**

Question 2

(a) Extracting `tar`-files changes the owner of the extracted files to be the user who runs the extraction program. Which attack is prevented by this measure? Justify your answer. **[10 marks]**

(b) `ssh` refuses to accept public keys for authentication of the user if the `.ssh` directory is accessible by anyone except the user or the file `.ssh/authorized_keys2` is not owned by the user or is writeable by others. Assume that firstly, `ssh` only checks that the file `.ssh/authorized_keys2` is not writeable by others, secondly that the `.ssh`-directory for Alice is writeable by everyone and finally that Bob can login into this host. Is it possible for Bob to login into this host as Alice? Justify your answer.
[10 marks]

Question 3

(a) Consider an openvpn-connection using TLS with forward secrecy for encrypting the traffic sent over the VPN. Assume you have access to the private key of the openvpn server and managed to extract a transcript of the encrypted traffic over the VPN.

(i) Why can you not decrypt the messages contained in the transcript?

(ii) What would malware running on the openvpn server need to add to the transcript to make it possible to decrypt the messages contained in the transcript? Justify your answer. **[10 marks]**

(b) 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]**