Two hours

UNIVERSITY OF MANCHESTER
DEPARTMENT OF COMPUTER SCIENCE

Cryptography and Network Security

Date: Monday 20th January 2020

Time: 14:00 - 16:00

Please answer all THREE Questions
Each question is worth 20 marks

Please use a separate answerbook for each Question

This is a CLOSED book examination

The use of electronic calculators is NOT permitted

1 Suppose the following is *Cathy*'s entry in the password file of Unix Server *Bob*.

```
Croe: 14mo31bmRY0Yg: 12:31:Cathy Roe: /home/croe:/bin/csh
………………………………………………..
```

Password file
on server

Answer the following questions.

(a) Describe the user authentication process used in Unix, i.e. the process by which the server *Bob* authenticates the user *Cathy*. In your description, you should also outline the input required by the authentication algorithm. (6 marks)

(b) Explain what a dictionary attack is in this context, and name two measures that are used by the Unix system to counter this attack. (5 marks)

(c) Explain what a replay attack is, how such an attack may be mounted in this context and what countermeasure the Unix system takes to thwart the attack. Can the countermeasure prevent replay attacks completely? Justify your answer. (5 marks)

(d) *Eve* spends *T* minutes attempting to guess a password of length *L* (characters) from an alphabet of *S* different characters. If *R* is the number of bytes per minute that can be sent over the communication channel linking the authentication server and *Eve*'s machine, and *N* is the number of characters exchanged when logging in, derive an equation to calculate the probability of success. (4 marks)

2 Alice is going to send a signed email to Bob. To allow Bob to verify her signature on the email, Alice will need to acquire a X.509 public-key certificate from a certification authority (CA) remotely via the Internet. Assuming that the key generation task is performed by Alice, answer the following questions.

(a) What is a public-key certificate? Outline the mandatory fields of an X.509v3 certificate. Name and justify two different application areas each with a different security requirement, in which the use of a public-key certificate is necessary.

(4 marks)

(b) Design a certificate acquisition protocol by which Alice could submit her public key to a CA, and obtain an X.509 certificate for the public key from the CA securely. You should give a step-by-step description of the protocol, including any verification that is respectively performed by Alice and CA.

(6 marks)

(c) Identify at least ***three*** security threats in this certificate acquisition process, and explain how the protocol described in (b) addresses these threats.

(6 marks)

(d) Outline ***all*** the necessary verifications that ought to be performed by Bob when he receives the signed email from Alice in order to be assured of the authenticity of the email.

(4 marks)

3 RSA and AES (Advanced Encryption Standard) are two different types of ciphers. You are now given two large primes, *p* and *q*, a cryptographic hash function *H*(*x*). Answer the following questions.

(a) Describe the RSA algorithm. In your description, you should make clear how RSA keys are generated, how a message is encrypted and how a ciphertext is decrypted.

(6 marks)

(b) Describe how, with the use of RSA, a digital signature on a long message, M, is generated and how the signature is verified. Identify three factors or considerations that should be considered to ensure the security of the signature generated.

(5 marks)

(c) There are four basic stages of operations, or called transformations, that are used to form the AES cipher. Briefly describe these four basic stages of operations.

(4 marks)

(d) Design an encryption method for Alice to send a long video stream*, V*, to Bob in a confidential manner over a communication network. In your method, you should make clear which cipher(s) are used and the mode of encryption. Justify your design.

(5 marks)

END OF EXAMINATION