University of Glasgow

Monday 13 May 2019
9:30 am – 11:00 am
(Duration: 1 hour 30 minutes)

DEGREE of MSc

Cryptography and Secure Development (M)

(Answer All Questions)

This examination paper is worth a total of 60 marks

The use of a calculator is not permitted in this examination

INSTRUCTIONS TO INVIGILATORS

Please collect all exam question papers and exam answer scripts and retain for school to collect. Candidates must not remove exam question papers.

1. (a) Explain why a system of arithmetic based on integers mod n, where n is a positive integer, is useful in encryption. Produce multiplication tables for integers mod 7 and integers mod 8 and use them to explain one weakness of modular arithmetic.

[5]

(b) A message consists of a series of 8-bit ASCII characters. An encryption scheme uses integers mod n=100,000,007 (a prime number). The encryption key e and the decryption key d are random numbers between 2 and n-1. Encryption consists of multiplying by e and decryption multiplying by d. What equation must e and d satisfy? How would you encrypt plaintext P, producing ciphertext C?

[5]

(c) Explain why an arithmetic system using polynomials with coefficients that are either 0 or 1 is more useful than integers mod n for encrypting bitstrings. Show with an example how it is possible to convert a bitstring into a polynomial and back again. How is multiplication defined to make sure that the polynomials don't become too large?

[5]

2. An encryption algorithm converts letters to and from numerical codes between 0 and 25 as follows: a=0, b=1, c=2, d=3, e=4, f=5, g=6, h=7, i=8, j=9, k=10, l=11, m=12, n=13, o=14, p=15, q=16, r=17, s=18, t=19, u=20, v=21, w=22, x=23, y=24, z=25. The encryption and decryption algorithms use arithmetic mod 26 on the numerical codes. A literature based running key algorithm encrypts English plain text using an English language key which contains the same number of letters as the plaintext. The key is taken from a book that is widely available in libraries. Corresponding letters are added modulo 26 for encryption and subtracted modulo 26 for decryption.

Try and deduce part of the plaintext and key if the corresponding letters in the ciphertext are **lom**. You may assume that high frequency letters are [aehot].

[7]

3 An organisation has decided to use a public key system that is similar to the RSA system. The only difference is that it uses integers mod n where n is the product of **three** primes not two. This is the only difference. Describe the encryption and decryption operations and show that one is the inverse of the other. State the public and secret keys.

[8]

4. (a) What is a blockchain and why is it useful? Describe the structure of the blockchain used in BitCoin.

[5]

(b) In the BitCoin system, a large number of individuals and organisations have a copy of the BitCoin blockchain. Why isn't there just one copy? How does BitCoin make sure that all the copies are the same, and what happens if some are different? How is a malicious organisation prevented from entering fraudulent transactions into the blockchain to give themselves ownership of other people's BitCoins?

[5]

(c) Alice has a BitCoin with value 10 BTC and spends 7 BTC with Bob. Describe in detail how she does this. You should explain how Bob makes sure Alice owns the coin and has not already spent it.

[5]

.

5. (a) Give three examples of a SQL injection attack, explaining in each case how a naive implementation of the server program will allow the attack to succeed. In each case, show how better coding can prevent the attack from succeeding.

[6]

(b) A system authenticates users by storing an encrypted version of their passwords in a table indexed by their user ID. When a user logs in they first enter their user ID. This is used to retrieve their encrypted password, which is read into an array. The user then enters their password into another array. This password is then encrypted, with the encrypted version being stored in a third array. The newly calculated encrypted password is then compared with the version retrieved from the table and if they are the same the user is allowed into the system. Show with an example how a poor implementation of this system can allow an attacker to get into the system without knowing the user's password using a buffer overflow attack. How can this attack be prevented?

[5]

(c) What is a poisoned null byte attack? Give an example to explain the coding errors that allow it to work? How can it be prevented?

[4]