A Fake Crypto Exam Paper (CSN11117/102)

There will be four main questions in the exam. This study guide has two main sections. Section A will provide some sample questions for three of the question, and Section B provides the study guide for the fourth question.

Link: http://asecuritysite.com/csn11117/guide

Section A

Three questions in the test. Here are a few questions to get you thinking in the right direction.

Q1. Explain how public key provides both privacy and identity verification.

Q2. Explain how the *e* and *d* values are determined within the RSA method. What are the values that are distributed and which are kept secret?

Q3. Outline the importance of storing the salt value with the hashed value when storing hashed passwords.

Q4. Computing power increases each year. Outline the challenge this gives when protecting encrypted data.

Q5. What are the possible advantages of using stream ciphers over block ciphers?

Q6. Bob encrypts his data using private key encryption and sends it to Alice. Every time he produces the ciphertext it changes, and he is worried that Alice will not be able to decipher the cipher text. He encrypts "Hello" and gets a different cipher stream each time. Why does the cipher text change?

Q7. Bob is sending encrypted data to Alice, and Eve is listening. After listening for a while, Eve is able to send a valid encrypted message to Alice. By outlining ECB, discuss how this might be possible.

Q8. Bob is using a password to generate a 128-bit encryption key. Explain why the key space is unlikely to be 2^128, and why key entropy could be used to measure the equivalent key size.

Q9. Bob has just produced a key pair, in a Base-64 format, and now wants to send this to Alice. What advice would you give him on sending the key pair to Alice?

Q10. Bob sends an encrypted message to Alice, and also sends his digital certificate to Alice to prove his identity. How does Alice prove that it is Bob who sent the message?

Q11. Eve has captured a hashed password. How might she use the Cloud to be able to crack the hashed password, and what is a likely tool for this?

Q12. Bob is an administrator for a network, and he tells his management team that user passwords are now salted, and they are thus completely secure against attacks. Is he correct? Explain your viewpoint.

Q13. Bob looks at the **passwd** file on his server, and wants to know the type of salting that is used. How would he do this?

Q14. Bob is looking for a new hashing method for storing passwords, and thinks that he will pick the fastest one. Is this a good approach? Explain your answer.

Q15. What are the typical tools that are used to crack hashed passwords, and what are the methods they will use to crack them?

Q16. Bob has two numbers which give a GCD of 1. Trent says that this happens because the numbers are prime. Is Trent correct? Explain your answer.

Q17. For Diffie-Hellman: G=2351; N=5683; x=7 and y=14. What is the shared key?

Q18. If we have a 16-bit key, but only use 200 phrases. What is the key entropy?

Q19. If it takes 10ns to test an encryption key. How long will it take to crack a 20-bit key?

Q20. With RSA, Bob selects two prime numbers of: p=3, q=5. What are the encryption and decryption keys? For a message of 4, prove that the decrypted value is the same of the message.

Q21. With Diffie-Hellman, G is 1579, and N is 7561. Bob selects 13 and Alice selects 14. Prove that the shared key is 868.

Q22. Bob selects a *p* value of 7 and a *q* value of 9, but he cannot get his RSA encryption to work. What is the problem?

Q23. Bob has selected a p value of 11 and a q value of 7. Which of the following are possible encryption keys: (5,77), (3,77), (9,77), (11,77), and (24,77).

Q24. Bob and Alice decide to use RSA encryption to send secure email, where Bob uses Alice's public key to encrypt, and she uses her private key to decrypt. What is the main problem caused with this, as apposed to using symmetric encryption?

Q25. Bob tells Alice that she should send her private key in order that he should encrypt something for her. Outline the main problem caused by this.

Q26. Security professionals say that RSA keys of over 1,024 bits are secure. What is the core protection against the RSA method being cracked for keys of 1,024 bits and more.

Q27. Bob and Alice get into a debate about the size of the d and e values in the RSA encryption key. Bob says that, in real-life keys, the length of the e value in (e,n) is normally about the same size as the d value (d,n). Alice disagrees. Who is correct?

Q28. Bob says that the number of bytes used for the cipher text will change directly with the number of bytes used in the plain text. Alice disagrees and says that most encryption methods involve having block sizes. Who is correct? Explain why.

Q29. With block encryption, how do we know where the ciphered data actually ends? Does it just use an end-of-file character or a NULL character?

Q30. Alice says she is confused that Bob is sending her the same message as a cipher, but every time the cipher text changes. Apart from using the shared encryption key, what does Alice use to decipher the cipher text?

Q31. Why would Eve have an aversion to salt?

Q32. Bob tells Alice that she won't be able to view the cipher text, but when she looks at the messages, they seem to be full of printable characters. What format is Bob likely to be using for the encoding of the cipher text, and what would you ask Alice to look for, in order to confirm your guess?

Q33. Alice has been reading her crypto books, and she reads that there should be an '=' symbol at the end of the encoding. She observes her encoding of cipher messages to Bob, and sees that some do not have an '=' sign at the end. Is there a problem with her encoder? If not, how often, on average, should she see an '=' sign at the end of her ciphered messages?

Q34. It was stated in the recent Yahoo hack that:

"We have confirmed, based on a recent investigation, that a copy of certain user account information was stolen from our networks in late 2014 by what we believe is a state-sponsored actor," Lord wrote. "The account information may have included names, e-mail addresses, telephone numbers, dates of birth, hashed passwords (the vast majority with bcrypt), and, in some cases, encrypted or unencrypted security questions and answers."

Do you think the vast majority of the hashed passwords will be cracked? Do you think they had good practice in place for hashed passwords?

Q35. You are working with a security consultant, and he says that you don't need to check the hashing of passwords, as it should work without testing. You disagree with him, and decide to test your hashing method. Initially you must find test vectors for MD5, SHA-1 and SHA-256. Can you find three test vectors, and test them against an on-line calculator?

Q36. At a security presentation a researcher gives a demonstration of Scrypt. In the presentation he shows a demonstration with a password of "password" and fixed salt of "NaCl". For each run he runs the hashing function, the hashed value changes, but, each time, the computation took longer. Which parameter is the researcher likely to be changing, and why does that parameter exist? Can the researcher select any value for the parameter? [Example]

Q37. There has been a major data breach within your company, and you are to appear on Sky News to report it. Your company has used PBKDF2 to hash its passwords. How do you explain to your customers that their passwords are unlikely to be breached?

Section B: Authentication, Identity and Trust

One question in the test. Here are a few questions to get you thinking in the right direction.

Q1. In the context of Access Control, explain subject, object and operation with the support of an example.

Q2. In the context of Access Control, identify which one is correct:

a) It is possible to have a system that does Authentication without Authorisation.

b) It is possible to have a system that does Authorisation without Authentication.

c) Authorisation must follow Authentication.

d) Authorisation (A2) is less important than Authentication (A1).

e) No authentication means no confirmation of subject’s identity thus no authorisation.

Q3. In the context of web application authentication, explain which username and password system is the most popular mechanism.

Q4. In the context of web application authentication, explain three threats for basic built-in HTTP authentication system for username and password system.

Q5. In the context of Access Control, explain why do we need to re-authenticate a user continuously in every request to a protected resource?

Q6. In the context of securing web authentication mechanism, explain how “allow account lockout” could be abused? What would be the countermeasures for this?

Q7. In the context of securing web authentication mechanism and with the support of an example explain how “allow accounts to be disabled” could reduce potential attacks surface.

Q8. In the context of determining access, compare ACL-based authorisation with role-based authorisation with the support of an example.

Q9. Traditional computer security was only concerned with the vertical directions explain how web application security adds the horizontal direction.

Q10. Illustrate your understanding of multi-factor authentication and two-step verification by considering this scenario:

A crazy navy submarine commander wants to start a nuclear war. He arrives at the secret port where his nuclear submarine is docked, enters the facility by flashing his military ID to the gate’s guard. He then boards the submarine, after being greeted by his subordinate sailor guarding the submarine’s ramp. Later the submarine sails and the commander instructs the crew to launch a nuclear missile against a foreign

country target. The foreign country retaliates, leading to the destruction of human civilisation.

In the scenario above:

a) List all the possible authentication factors and explain/relate them with the above scenario

b) Commend on whether each of the factors is effectively and what the problems may be?

c) How would you improve the authentication system?

d) What could be done to prevent crazy commanders cannot start nuclear wars?

Explain your answer while demonstrating your knowledge in the area and stating any assumptions you may make.

- CSN11117/CSN11102 fake exam questions (2017). Any questions? Ask Bill (Skype: billatnapier).