Applied Crytograpy and Trust Test 1 (CSN11131)

There will be four main questions in the exam.

- Symmetric Key.
- Hashing.
- Public Key/Digital Certificates.
- Key Exchange.

These are some sample questions which will get you thinking in the right direction.

1. Symmetric Key

Key principles: Salting, AES, ECB, CBC, Hashing

Q1 Computing power increases each year. Outline the challenge this gives when protecting encrypted data. [Ref: Symmetric Key]

Q2 What are the possible advantages of using stream ciphers over block ciphers? [Ref: Symmetric Key]

Q3 The AES method is recommended by NIST for symmetric key encryption. What are the main stages involved in the AES process? [Ref: Symmetric Key]

Q4 Bob encrypts his data using symmetric 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? [Ref: Symmetric Key]

Q5 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. [Ref: Symmetric Key]

Q6 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. [Ref: Symmetric Key]

Q7 Bob uses a six-character password with lower case [a-z]. How many passwords are possible? His password system then tells him he needs to add numeric value [0-9]. If he adds it at the end, how many passwords are possible, and what is the key entropy? [Ref: Symmetric Key]

Q8 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. [Ref: Symmetric Key]

Q9 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? [Ref: Symmetric Key]

Q10 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? [Ref: Symmetric Key]

Q11 Why would Eve have an aversion to salt? [Ref: Symmetric Key]

Q12 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? [Ref: Symmetric Key]

Q13 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? [Ref: Symmetric Key]

2. Hashing

Q14 Outline the importance of storing the salt value with the hashed value when storing hashed passwords. [Ref: Hashing]

Q15 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? [Ref: Hashing]

Q16 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. [Ref: Hashing]

Q17 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? [Ref: Hashing]

Q18 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. [Ref: Hashing]

Q19 What are the typical tools that are used to crack hashed passwords, and what are the methods they will use to crack them? [Ref: Hashing]

Q20 If we have a 16-bit key, but only use 200 phrases. What is the key entropy? [Ref: Hashing]

Q21 If it takes 10ns to test an encryption key. How long will it take to crack a 20-bit key? [Ref: Hashing]

Q22 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? [Ref: Hashing]

Q23 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? [Ref: Hashing]

Q24 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] [Ref: Hashing]

Q25 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? [Ref: Hashing]

3. Public Key

Key topics: RSA, Elliptic Curve

Q26 Explain how public key provides both privacy and identity verification. [Ref: Public key]

Q27 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? [Ref: Public key]

Q28 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? [Ref: Public key]

Q29 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. [Ref: Public key]

Q30 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. [Ref: Public key]

Q31 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? [Ref: Public key]

Q32 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). [Ref: Public key]

Q33 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? [Ref: Public key]

Q34 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. [Ref: Public key]

Q35 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. [Ref: Public key]

Q36 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? [Ref: Public key]

Q37 Bob says that Elliptic Curve Cryptography (ECC) is an easy method to crack. Explain to Bob how ECC operates, and why it can be a secure method. [Ref: Public key]

4. Key Exchange

Key topics: Diffie-Hellman, ECDH, Using Public Key to Exchange Key

Q38 For Diffie-Hellman: G=2,351; N=5,683; x=7 and y=14. What is the shared key? [Ref: Key Exchange]

Q39 With Diffie-Hellman, G is 1579, and N is 7561. Bob selects 13 and Alice selects 14. Prove that the shared key is 868. [Ref: Key Exchange]

Q40 Eve says that she sees the values passed within ECDH by Bob, and that she can crack the key. By explaining the ECHD key exchange method, outline how it would likely to be difficult for Eve to determine the shared key. [Ref: Key Exchange]

Sample Exam paper from past

This exam paper was a closed book test.

Question 1

Bob and Co is an ISP, and they have recently been hacked, and their passwords released to the Internet. Their lead Information Officer defines that the passwords use eight-character passwords and were salted with a three-character hex value. The regular expression to filter the passwords defines the range of [a-z0-9] with a letter of the alphabet in the first character.

(a) What advice would you give to the company on their current policy on hashing their passwords? [5]

(b) In the investigation, a hash cracker of 1 Tera hashes per second has been used. Can you estimate how long it would take to crack all the passwords in the data? Give the working-out. [5]

Question 2

(a) Calculate, for Diffie-Hellman, the shared key, if the agreed values are G=201, N=31, and Bob selects 15 and Alice selects 3. Give the working-out. [Marks: 3].

(b) In RSA, Bob generates two prime numbers: 13 and 11. From this create the encryption and decryption key. Give the working-out. [Marks: 3]

(c) Mallory and Eve are being watched by law enforcement agencies. The law enforcement agency decides that they want to decrypt the messages sent by Mallory to Eve, and thus sends Mallory a digital certificate related Eve, with a fake public key (for which they have the private key). Outline the problems that could be caused by this method, and how might the law enforcement agency overcome them? [Marks: 4]

Question 3

(a) PKI uses key pairs for encryption and digital certificates to prove identity. Explain how PKI can be used to keep messages between Bob and Alice secret, and also how we can prove Bob's identity and the integrity of the message. How might an intruder manage to pretend to be Bob? [Marks: 5]

(b) PGP provides a method of securing email. Outline how PGP uses asymmetric and symmetric encryption in order to secure emails, while proving identities. [Marks: 5]

Question 4

(a) Outline the main weaknesses of passwords which use hashed values, and how salting overcomes these problems. How might a hacking tool overcome the usage of salt? [Marks: 5]

(b) For the following salted password (128-bits of salt) outline the process that would be involved when the user logs-in, and how the password would be checked. [Marks: 5]:

$2a$06$NkYh0RCM8pNWPaYvRLgN9.LbJw4gcnWCOQYIom0P08UEZRQQjbfpy