**Ciphers and Fundamentals**

* 1. **Using the table [**[**here**](https://asecuritysite.com/public/test_table.pdf)**], what is the Base-64 encoding for "test"?**
  2. **Using the table [**[**here**](https://asecuritysite.com/public/test_table.pdf)**], is the Base-64 encoding for "help"?**
  3. If it takes 1ns to test an encryption key. How long will it take to crack a 32-bit key?
  4. If it takes 10ns to test an encryption key. How long will it take to crack a 20-bit key?
  5. 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?
  6. 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?
  7. **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.**
  8. **Bob deals in Bitcoins and tells Alice that he has a Base-58 ID? Alice says he is crazy, and has only heard of Base-64. What is Base-58 and how does it differ from Base-64?**
  9. **Bob encrypted a message in 1980, and it took a million years to crack at the time. Assuming that computing power doubles each year, do you think the message will be safe against cracking for existing computer systems?**

**Symmetric Key**

* 1. **Explain the differences between stream and block ciphers, and why salt is required within the encryption process.***Where would I find this info?* Have a look at the penguin in [Unit 2](https://asecuritysite.com/public/chapter02_secret.pdf) (Slide 15 and on), and here's an outline of the problem with ECB in this related [article](https://medium.com/asecuritysite-when-bob-met-alice/when-is-high-grade-encryption-not-high-grade-when-its-ecb-e1509ec56930?source=friends_link&sk=31ec28f1c2be74a81e53c67e71d5b259).
  2. What are the possible advantages of using stream ciphers over block ciphers?
  3. Bob encrypts his data using secret key encryption and sends it to Alice. Every time he produces the cipher text 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, and why is she still able to decrypt it, even though it changes each time?
  4. **AES uses an S-box to scramble the bits. How are the S-boxes for the encryption and decryption process linked?**
  5. 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. Where would I find this info? Have a look at the penguin in [Unit 2](https://asecuritysite.com/public/chapter02_secret.pdf) (Slide 15 and on), and here's an outline of the problem with ECB in this related [article](https://www.linkedin.com/pulse/when-high-grade-encryption-high-grade-its-ecb-william-buchanan).
  6. 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. Where would I find this info? This is related to key entropy [here](https://moodle.napier.ac.uk/encryption/en), and try and understand how key entropy relates to the strength of the encryption.
  7. 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.
  8. 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?
  9. 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?
  10. 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?
  11. **Which of these is correct for CMS padding: "68656c6c6f3132330808080808080808", "68656c6c6f3132330909090909090909", and "68656c6c6f3132330A0A0A0A0A0A0A0A".**   
      *Where would I find information on this?* Look [[here](https://asecuritysite.com/encryption/padding)]
  12. **Bob wants to cipher "edinburgh" with the key of "hello123" for a 256-bit AES key, and his encoding gives him "6564696e6275726768". What will be the padding that will be added?**
  13. **Eve says she thinks she can determine the number of characters within some ciphered plain-text. Is she correct? If so, how many plain-text characters were there in this ciphered message:** "6920776f756c64206c696b6520746f2074616b65206120627265616b04040404".
  14. **RC4 is a stream cipher, which is one of the recommended ciphers for IoT devices. Bob says that it has an infinitely long encryption key, and that his devices will not be able to cope with this size of key. How would you convince him that IoT devices will be able to cope with RC4?**
  15. **RC4 is used within Wifi systems. With WEP, a 40-bit encrytion key which was shared over the network, and which had a 24-bit IV value. In relation to the key size, the scope of the key, and the size of the IV, what do you think were the fundamental problems with this setup?**
  16. **Bob says that he can created two ciphers from a file with the word "hello", and which will always create the same cipher. If the cipher is "Z8onq9tXC3CL2oOwqLLWbg==" and the key is "password", which is the missing part of the command he used (find the replacement for [OPTION1] and [OPTION2]):**  
        
       openssl enc -e -[OPTION1] -in test.txt -pass pass:password -nosalt -[OPTION2]
  17. **The following are encrypted with aes-256-cbc or 3-DES and have a password of "napier", "123456" or "password". Decode them:**  
        
      U2FsdGVkX18K9Dy9I/CewpNH2svvjyhNG3Bod77+uYo=  
      U2FsdGVkX18pmUpnI7iopG3gsHVQPT1zyRwjlvAJ+aI=  
      U2FsdGVkX19XlsCN50CFxZlBcCplPs9/  
        
      **Please note: In the file you create, put one new line after the Base64 text. For example the answer to the first one is:**  
      openssl enc -d -aes-256-cbc -in test.txt -pass pass:123456 -base64

**Hashing and MAC**

* 1. Outline the importance of storing the salt value with the hashed value when storing hashed passwords.
  2. 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.  
     Where would I find this info? This is related to key enthropy [here](https://asecuritysite.com/encryption/en), and try and understand how key enthopy relates to the strengh of the encryption.
  3. 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?  
     Where would I find this info? Have a think about the certificate which is distributed. You can observe it [here](https://youtu.be/GLOObdTy5uY)
  4. **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?**
  5. 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 too for this?  
     *Where would I find this info?* This [article](https://www.linkedin.com/pulse/quantum-v-supercomp-cloud-gpu-race-ultimate-cracking-william-buchanan) outlines a number of methods which might be used, included within Cloud cracking.
  6. 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.  
     Where would I find this info? Have a read of the following [article](https://www.linkedin.com/pulse/salting-password-only-secure-when-you-keep-salt-secret-buchanan?forceNoSplash=true).
  7. 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?  
     *Where would I find this info?* Have a quick look at the additional lab on [Software Hashes](https://asecuritysite.com/lab04_software_hash.pdf). If you can get the Python script to run in Section G, you'll see them all.
  8. 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.  
     Where would I find this info? Think about whether being fast for hashing is a good idea. Have a look at this [article](https://www.linkedin.com/pulse/when-slow-good-great-slowcoach-bcrypt-william-buchanan). But make up your own mind on the subject.
  9. What are the typical tools that are used to crack hashed password, and what are the methods they will use to crack them?  
     *Where would I find this info?* Unit 3 and [Lab 2](https://asecuritysite.com/lab03_hashing_and_certs.pdf)
  10. Why would Eve have an aversion to salt?
  11. **A password is defined as [a-z]. For a four character password, show that there are 456,976 different passwords.**  
      *Where would I find this info?* Have a look [here](https://asecuritysite.com/encryption/passes).
  12. **A password is defined as [a-zA-Z]. For a four character password, show that there are 7,311,616 different passwords.**  
      *Where would I find this info?* Have a look [here](https://asecuritysite.com/encryption/passes).
  13. **A password is defined as [a-zA-Z0-9]. For a four character password, show that there are 14,776,336 different passwords.**  
      *Where would I find this info?* Have a look [here](https://asecuritysite.com/encryption/passes).
  14. It was stated in the recent Yahoo hack [that](https://arstechnica.co.uk/security/2016/09/yahoo-says-half-a-billion-accounts-breached-by-nation-sponsored-hackers/):  
      "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?

* 1. 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?

* 1. 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](https://asecuritysite.com/encryption/scrypt)]

* 1. 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?

**Asymmetric Encryption (Public Key)**

* 1. 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?
  2. 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).
  3. 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 opposed to using symmetric encryption?
  4. 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.
  5. 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?
  6. **Bob says he has had a look at a few RSA public keys and he says that the ones he looked at where all the same. Is he right? If so, what makes public keys different?**
  7. **Research: Netscape had to comply with an export** [**embargo**](https://en.wikipedia.org/wiki/Export_of_cryptography_from_the_United_States) **on the size of the keys which can be used for RSA. Which major vulnerabilities have resulted?**
  8. 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?  
     *Where would I find this info?* Have a look at some practical examples: [Here](https://moodle.napier.ac.uk/encryption/rsa2)

**Key Exchange**

* 1. **Eve listens to Bob and Alice's communication for their Diffie-Hellman handshaking. In order to generate the same key as Bob and Alice, which values will Eve try to determine, and how is it likely to be difficult to gain these?**
  2. For the following key exchanges, Bob generates x, and Alice generates y. Prove the shared key. [[Examples](https://asecuritysite.com/public/diffie_examples.pdf)]  
       
     x=3, y=4, G=4 and N=7. Share=1.  
     x=6, y=15, G=5 and N=23. Share=2.  
     x=5, y=7, G=10 and N=541. Share=193.  
     x=6, y=15, G=5 and N=23. Share=2.  
     x=7, y=7, G=5 and N=11. Share=9.  
     x=7, y=9, G=8 and N=13. Share=5.  
     x=5, y=4, G=2969 and N=9929. Share=8106.  
     x=6, y=5, G=3881 and N=125. Share=792.  
     x=3, y=4, G=3623 and N=1153. Share=939.
  3. **Why are Forward Security and Ephemeral so important for the security of your keys?**

**Digital Certificates**

* 1. **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?**  
     *Where would I find this info?* Have a think about the certificate which is distributed. You can observe it [here](https://youtu.be/GLOObdTy5uY)
  2. **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?**