**Section 3**  
Explain how public key provides both privacy and identity verification *2 keys a private key and a public key. Privacy can be achieved by using the public key to encrypt the data and then send to the key owner, and then that can only be decrypted using the public key. This is useful for an exchange of a symmetric key for large scale data transfers. Identify verification can be done by encrypting the text with the private key and as this can only be decrypted by the public key from Bob, this means only Bob could have encrypted the message, thus proving Bob's identity.*  
   
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? *p and q are two prime numbers times together to create n, which is the modulus. P and q then each have 1 minused away from them and then times together to create PHI. E is then randomly selected from a number from between 1 and PHI that is not a factor of PHI. The e value is then worked out via an inverse mod, so that (d x e) mod n = 1.*  
*The [e, n] value is shared which is the public key*  
*The [d, n] value is kept secret, which is the private key.* **Note to ask: Bill - Fermat prime**  
   
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? *Our advice would be to not send the key pair. Base64 is only an encoded technique and so it could be reverse engineered. Only send the public key unless they really need to send the key pair. If that’s the case then the key pair would need to be encrypted via another already established encrypted traffic.*  
   
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. *Trent is incorrect, the two numbers are in fact co-prime. This means that the numbers that share no common factors aside from 1. The numbers do not have to be prime numbers.*  
[*https://asecuritysite.com/encryption/gcd*](https://asecuritysite.com/encryption/gcd) *- useful for determining the GCD.*  
   
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. *e = [7, 15]*  
*d = [7, 15]* **Need to bring this up with Bill. Because the message is the same value as the encrypted text.**  
   
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? *9 is not a prime number.*  
   
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). *PHI is 60 because (p-1) x (q-1) = 10 x 6 = 60*  
*The factors of PHI are 1 2 3 4 5 6 10 12 15 20 30 60.*  
*The factors of 5 are 1 and 5.*  
*The factors of 3 are 1 and 3.*  
*The factors of 9 are 1, 3 and 9.*  
*The factors of 11 are 1, and 11*  
*The factors of 24 are 1, 2, 4, 6, 12, and 24.*  
*So because 11 is the only one that does not share a factor with 60 aside from the factor of 1 the only valid encryption key is (11, 77) because the other 4 share common factors with PHI which is 60.*  
   
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? *RSA is a public key encryption method. The main problems with public key encryption methods are that they are much slower in terms of performance.* **Note: Talk to Bill about this to confirm which is the "main problem" and what are the other problems.**  
   
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. *The problem is Bob. The main problem with this is that this does not really provide encryption of data. What it is doing is allowing the file to be encrypted so that anyone can then decrypt it with her public key. This means that everyone would believe the file came from Alice, and thus she would be the responsible party for any problems with the data. Additionally, it means Bob could encrypt any other files in the future and pretend to be Alice.*  
   
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. *The core protection against the RSA method being cracked is integer factorisation which is that it’s currently computational difficult to compute a prime number of greater than 768bits. However, state actors may have more resources which is why it is currently being recommended to move to 2048 bits.*  
   
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? *Bob is incorrect. While it is possible to have e and d values be of the same size, in real-life practice the e value of 65537 is chosen in order to make the public key verification much quicker, and allows for choosing a much larger d value which makes it more difficult to compute the d value from the e value.* **Note: talk to Bill to discuss whether an e and d value can be the same size. Also what does it mean by "size".**  
   
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. **Note: Talk to Bill to explain this one.**  
   
**Section 4. Key Exchange**  
   
For Diffie-Hellman: G=2,351; N=5,683; x=7 and y=14. What is the shared key? *g value is:    2351*  
*p value is:    5673*  
*a value is:    7*  
*b value is:    14*  
*A value is:    770*  
*B value is:    2908*  
*Ba value is:   3931*  
*Ab value is:   3931*  
*Shared key = 3391*  
   
With Diffie-Hellman, G is 1579, and N is 7561. Bob selects 13 and Alice selects 14. Prove that the shared key is 868.  
   
*g value is:    1579*  
*p value is:    7561*  
*a value is:    13*  
*b value is:    14*  
*A value is:    37*  
*B value is:    5496*  
*Ba value is:   868*  
*Ab value is:   868*  
*Shared key = 868*  
   
Eve says that she sees the values passed within ECDH by Bob, and that she can crack the key. By explaining the ECDH key exchange method, outline how it would likely to be difficult for Eve to determine the shared key. *Eve is incorrect because ECDH relies on the discrete logarithmic problem which is a computational difficult problem. Because the original values from both sides are not capturable by Eve, she misses crucial information for her to be able to decode the x and y values generate by Alice and Bob respectively.* **Note: Ask Bill for more detail.**  
   
**Previous Exam Questions**  
   
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] *Longer salt, as they are only using 3 characters for salt it means they are not using a slow hashing algorithm, so they should implement a slow hashing algorithm such as Bcrypt PBKDF2 to slow down the cracking of hashed passwords.*  
*Other aspects that can be looked at are increasing the password length to length to a minimum of 11 characters. Add in upper case characters as well as special characters. Remove the alphabetical character from the first position.* **Note: Ask Bill is the question asking about hashing only, or does it include other aspects such as increasing password length.**  
   
(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] *Because there is an alphabetical character in the first position this provides 26^1 possible combinations. For the other 7 values they can be lower case characters and numbers which gives 36^7 possible combinations. Additionally the three-character hex values as salt provides 16^3 possible combinations.*  
  
*Assuming the salt was not stolen with the password this provides 8.345x10^15 possible combinations. With 1 terahash per second this means that it would be cracked in 8,345 seconds, which works out at approximately 2h10mins.*  
  
*If the hash was stolen then means there are only 2.0x10^12 which means it can be cracked in 2 seconds.*  
   
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]. *g value is:    201*  
*p value is:    31*  
*a value is:    15*  
*b value is:    3*  
*A value is:    30*  
*B value is:    27*  
*Ba value is:   30*  
*Ab value is:   30*  
*Shared key = 30*  
   
(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]  
   
*n = p x q = 13 x 11 = 143*  
*PHI = (p-1) x (q-1) = 12 x 10 = 120*  
*e = A number between 1 > 120 that does not share a factor of PHI. 97 was selected.*  
*d = A co-prime of e with a GCD of 1 = 73*  
*Encryption key = [e, n] = [93, 143]*  
*Decryption key = [d, n] = [73, 143]* **Note: ask bill how he would like this express mathematically.**  
(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] *If the LEOs are not acting as MITM Eve will be receiving encrypted data which she can't decrypt and make her and Mallory aware that they are being monitored. They could then start feeding false information to the LEOs.*  
*The certificate that Eve has may be signed by her private CA which the LEOs would not have access to, and this means that Mallory would know there was a false certificate.* **Note: Ask Bill what other problems there could be..**