Examiners' commentaries 2016–17

CO3326 Computer security – Zone A

General remarks

The written examination comprised five questions, of which candidates were required to answer three. The time allowed was two hours fifteen minutes. Candidates are reminded to carefully plan their time in the examination in order to allow sufficient time to complete all of the questions and to show their workings.

Comments on specific questions

Question 1

a. This required candidates to generate a shared secret key using the Diffie-Hellman key exchange protocol. Most candidates found this straightforward, and showed their working to arrive at the answer: 9.

b. This required candidates to name and describe a method of key management that involves using a Trusted Third Party. Either Needham Schroeder or X.509 certification protocol were acceptable answers, and most candidates provided thorough descriptions. Marks were lost where candidates only offered symbolic description for Needham Schroeder, or where steps were missing or incorrect for the Certification protocol.

c. This required a description of the web of trust model for key management in PGP, and asked for one advantage and disadvantage compared with the method described for b). Most candidates provided sound explanations, covering legitimacy values. Good answers went on to offer lower cost, or reliance as an advantage, and time-consuming to maintain as a disadvantage.

d. This tested knowledge of the Bell LaPadula no-read up and no-write down rules. This is straightforward bookwork, but a few candidates became rather muddled, and would perhaps have benefited from re-reading their answers.

e. This elaborated on part 1d., requiring an explanation of why strict enforcement of the rules might cause problems for users, and the exceptions permitted in order to overcome these problems. Most candidates provided clear answers.

Question 2

a. This required the use of Fermat's Little Theorem with base 2 to show that 93 is not a prime number. This was generally answered very well.

b. This was bookwork; candidates needed to give the key generation protocol for the RSA public key cryptosystem, and most did so very competently.

c. This required encryption of a message using public RSA keys. Again, most candidates found this straightforward, providing a table to show their working to arrive at the answer: 19.

d. This required confirmation of the value of a private key. Some students found this too challenging, though two possible methods involve:

- factorisation of n – shown to be composite in a)
- decryption of answer to c) – or encryption/decryption of a new message.

e. This required an explanation of how and why RSA might be used to exchange a key for use in a symmetric key cryptosystem. Some candidates provided rather garbled accounts, sometimes omitting any verificatory step; some also overlooked the 'why' part of the question, though the answer is simply that it is slow and expensive to use RSA to encrypt long messages, compared to using a symmetric key cryptosystem.

Question 3

a. This required candidates to provide the decryption function (the encryption function is given in the question). Candidates generally either did this correctly, or simply did not attempt to answer this part.

b. Candidates who provided the decryption function correctly were generally able to explain that the multiplicative inverse requires that a and m are co-prime, and to provide the possible values.

c. This required the decryption of affine cyphertext. Good answers included step-by-step working, using the decryption function.

d. This required consideration of the relationship between Affine and Caesar cypher. Some candidates recognised that the Affine is a generalised Caesar cipher, but others got this the wrong way around.

e. This required candidates to explain the differences between three modes of operation for block cyphers. Answers were generally sound.

Question 4

a. This required an explanation of *n* of *n* key escrow protocol. Candidates generally provided clear accounts, and correctly suggested that it is rarely used as it requires all keyholders to get together to produce the key.

b. This required finding the value of a secret key in a 2 of 3 key escrow scheme, with two key pieces given. Answers here were mixed; while some candidates were able to produce the relevant equations, there was some confusion over which equation should be subtracted from which (perhaps because there are two alternatives). Partial marks were awarded where the working steps demonstrated a level of understanding.

c. This was essentially bookwork, requiring explanation of various concepts in the context of cryptographic hash functions. Some candidates ignored the context. It is essential to read questions carefully, to establish exactly what is being asked.

d. This required candidates to explain why two given functions were not cryptographically strong. Part i) was generally well answered – it would be easy to find two input values with the same *H* value; for example, 100 and 200 will both map to 0. Part ii) was answered less well – a very large value of *m* will have a correspondingly large *H(m)* value; or H(*m*) will be hard to compute; for example, if *m* has 1000 digits, then it would be hard to determine the m^{th} prime.

Question 5

a. and b. These parts required a simple explanation of the Elliptic Curve Discrete Logarithm Problem (ECDLP), and an associated calculation. These questions were based on the coursework, and should have been straightforward. Disappointingly, very few candidates were able to provide clear accounts.

c. This was bookwork, requiring candidates to write explanatory sentences for security features. This was generally done very well.

d. This explored security features in relation to hash functions. Some answers seemed rushed or even careless, possibly due to lack of time.

Examiners' commentaries 2016–17

CO3326 Computer security – Zone B

General remarks

The written examination comprised five questions, of which candidates were required to answer three. The time allowed was two hours fifteen minutes. Candidates are reminded to carefully plan their time in the examination in order to allow sufficient time to complete all of the questions and to show their workings.

Comments on specific questions

Question 1

a. This required candidates to provide the decryption function (the encryption function is given in the question). Candidates generally either did this correctly, or simply did not attempt to answer this part.

b. Candidates who provided the decryption function correctly were generally able to explain that the multiplicative inverse requires that *a* and *m* are co-prime, and to provide the possible values.

c. This required the decryption of affine cyphertext. Good answers included step-by-step working, using the decryption function.

d. This part required consideration of the relationship between Affine and Caesar cypher. The Affine is a generalised Caesar cipher, but several candidates got this the wrong way around.

e. This was answered very well by nearly all candidates, with clear explanations of statistical analysis and redundancy, and illustrative examples. Brute force was recognised as a last-resort technique, or for use where the keyspace is very small.

Question 2

a. and b. These parts required a simple explanation of the Elliptic Curve Discrete Logarithm Problem (ECDLP), and an associated calculation. These questions were based on the coursework, and should have been straightforward. Disappointingly, very few candidates were able to provide clear accounts.

c. This required an account of the four properties that a hash function should satisfy to be considered cryptographically strong, together with an explanation of their importance. This was generally done well, although some candidates lost marks by failing to explain the importance of each property.

d. This involved protocol design for a specific scenario, to enable a user to check a cloud storage provider keeps complete versions of their files as a backup. The user will also keep backups themselves. The files are too large to insist on seeing entire copies, so the protocol must involve a hash function. A variety of answers were offered, though many did not offer assurance that the provider was keeping complete versions. A simple protocol would be to send the provider a random salt value and ask them to return the value of *SHA512(salt || file)* where || means concatenation so $a \,||\, b = ab$. Their result could then be matched to that obtained locally, to

confirm they have kept the files. The key here is that different intermediate hash values will be used each time the check is performed, depending on the random salt.

Question 3

a. This part required the use of Fermat's Little Theorem with base 2 to show that 93 is not a prime number. This was generally answered very well.

b. This was bookwork; candidates needed to give the key generation protocol for the RSA public key cryptosystem, and most did so very competently.

c. This required encryption of a message using public RSA keys. Again, most candidates found this straightforward, providing a table to show their working to arrive at the answer: 38.

d. This part required confirmation of the value of a private key. Some students found this too challenging, though two possible methods involve:

   - factorisation of n – shown to be composite in a)
   - decryption of answer to c) – or encryption/decryption of a new message.

e. This required candidates to explain how Alice could encrypt and sign a message for Bob. Most found this straightforward. Some also included Bob's verification protocol, though this was not required.

Question 4

a. This required finding the value of a secret key in a 2 of 3 key escrow scheme, with two key pieces given. Answers here were mixed; while some candidates were able to produce the relevant equations, there was some confusion over which equation should be subtracted from which (perhaps because there are two alternatives). Partial marks were awarded where the working steps demonstrated a level of understanding.

b. This required an explanation of n of n key escrow protocol. Some candidates provided clear accounts, and correctly suggested that it is rarely used as it requires all keyholders to get together to produce the key.

c. This was bookwork, requiring candidates to explain how 3DES uses the DES algorithm with a 168-bit key. Many candidates answered this well.

d. This was also generally well answered, though some candidates got confused in explaining how the Feistel structure generates block input for the next round. Good answers typically used diagrams for clarification.

e. This was bookwork, and required an explanation of why Rijndahl allows different key sizes to be used. Short, simple answers were acceptable, relating to flexibility, criticality, speed and cost.

Question 5

a. This explored the El Gamal cryptosystem, and candidates showed a good level of familiarity in their explanations. It is important to show workings, as where slips are made, examiners can award partial credit.

b. This required candidates to describe the Needham Schroeder protocol. While there were some very good answers, this part was generally less well done, with steps muddled or missing, etc. Some answers seemed rushed, possibly due to lack of time.

c. This part asked candidates to explain why the PGP signature component and session component are required. Some candidates were able to make a reasonable attempt, but again, some answers were incomplete, again possibly due to lack of time.