E.44 Network Security Specimen Exam Paper 1 Answers

1 (i) Reverse rounds and keys (i.e. replace round 1 with round 16 and key1 with key 1 and configure round structure for decryption)
(ii) The weak keys are such that all per round keys are the same. The 4 weak keys are as follows:
28 zeros followed by 28 ones
28 ones followed by 28 zeros
56 ones
56 zeros (in the above the parity bits have been ignored)
(iii) An exhaustive key search is a test using all possible keys. In a search of the DES key space a number of 2 raised to the power of 56 would be required.
(iv) 3DES is encryption with key 1 followed by decryption with key 2 followed by encryption with key 1. Since the effective key length is 112 bits the strength is increased by 2 raised to the power of 56.
(v) Addition is reversed by adding the 16-bit output with the additive inverse of the key used in the original operation. Similarly multiplication is reversed by multiplying the result of the original operation by the key's multiplicative inverse.
It is always possible to find the additive inverse. Since 257 is prime it will also be possible to find the multiplicative inverse. Both operations are reversible.

2 (i) There are pq – 1 positive integers less than pq. In order to find Euler's function for n we need to remove those which are relatively prime to n. There are q-1 multiples of p and p-1 multiples of q in thid category. Euler's function for pq is therefore
$pq - 1 - (p-1) - (q-1) = pq - p - q + 1 = (p-1)(q-1)$
(ii) The message must be smaller than n because the operations are taken mod n and a message longer than n could not be distinguished from its value mod n.
The message may be deciphered by finding the normal cube root.
(iii) Refer to lecture handout for an explanation of Diffie-Hellman. An observer cannot (i.e. operation is computationally infeasible) find a from g raised to the a mod p.
(iv) Refer to lecture handout for an explanation of the bucket brigade attack and possible methods of protection

3 (i) A possible approach would be to use MD5 to form a digest of the message. The digest should then be signed with the private key of RSA. The message and signature should then be encrypted with CBC/IDEA.
(ii) If the RSA facility were not available source authentication could be provided by forming a keyed has of the message using MD5 and the IDEA key. Encryption would follow as before. This would not provide non-repudiation and it would generally be . weaker than the (i) regarding authentication as the same key has been used for authentication as encryption.
(iv) The proposed message digest function is a poor function since it would be relatively simple to find many messages with the same digest. Thus if the signature or MAC is known for one message it would be possible to reuse this signature or MAC for a number of alternative messages.

4 (i) Proof of submission is proof that a message was submitted to the electronic mail system. Non-repudiation enables a recipient of a message to prove in a court of law that it was sent by a particular sender. Non-repudiation in e-commerce prevents

initiators of transactions later claiming that the recipient or some other party made the transaction in their name.

(ii) IPSec would reject the packets and would not pass them to TCP. In SSL such packets could cause the session to break.
(iii) Refer to lecture handout
(iv) Refer to lecture handout. Kerberos does not provide Perfect Forward Secrecy since it uses master keys which are long term secrets.

5 (i) Refer to lecture handouts. It is possible to operate a public key security system without a PKI but there would be little trust in the public keys used.
(ii) Refer to lecture notes for (a) PGP, (b) web browsers and (c) PEM
(iii) Since recipients of the CRL would not know exactly when the CRL would be issued they would not be alarmed if it were intercepted and removed.

6 (i) First message is a comms request with the nonce N1. The nonce is included to prevent replay by an attacker who has obtained an old key of B. KDC's reply in the second message includes the returned nonce and provides a ticket encrypted under B's master key. It also includes a session key for a and B to communicate securely. All thgis information is secured by encryption under A's master key. In the third message A asses the ticket to B so that B can find the session key. To check whether B has done this correctly A also issues a challenge in the form of a number N2 which is sent encrypted under the session key KAB. The fourth message confirms that B has found N2 (which it proves by returning N2 – 1 encrypted under the session key) and also sets A a challenge with the number N3 encrypted under the session key. In the final message A responds to the challenge by returning N3 – 1 encrypted under the session key.. To summarise the functions of the numbers used in the protocol, N1 is to prevent replay whilst N2 and N3 are challenges in an authentication protocol.

(ii) In V4 each KDC must be registerd as a principal with every other KDC. A client's home KDC arranges a secure session with another KDC which can then arrange a secure session with a server registered with it as a principal.

(iii) In V5 the KDC's do not need to be registered as principals with all other KDCs but may communicate through a hierarchy of KDCs. Refer to lecture handouts for other differences between V4 and V5.

E4.44/ISE4.45/SO21 Answers to Sp[pecimen Exam Paper 2

1 (i) From the diagram

L(n+1) = R(n) and R(n+1) = L(n) + Mkn(R(n)) where + denotes bitwise exclusive or

Clearly R(n) = L(n+1) and by adding (exclusive or) Mkn(R(n)) to both sides of the second equation gives L(n) = R(n+1) + Mkn(R(n))
Refer to lecture handout to check your diagram for decryption.

(ii) 3DES is EDE with keys k1, k2 and k1 respectively. Effective key length is 112bits. The second operation is decryption rather than encryption to prevent the final permutation of encryption being reversed by the initial permutation of a second encryption. Two encryptions using k1 and k2 could be attacked by forming tables for a known plaintext/ciphertext pair of 64-bit blocks. The first table would contain the ciphertext for all possible keys used fro encrypting the plaintext. The second table would contain the results of deciphering the known ciphertext with all possible keys. By comparing the results for matches the attacker will find a number of possible matches. These are tried with other known plaintext/ciphertext blocks until a consistent set of matches is obtained. This attack requires considerable storage but is much less computationally intensive than an exhaustive key search.

(iii) Decryption requires the same operations with the additive inverse of kb and the multiplicative inverse of ka. The additive inverse of AC46 is 53BA. 0000 does not have a multiplicative inverse. In order to obtain a multiplicative inverse for this key it is interpreted as 2 raised to the power of 16.

(iv) In the following take + as bitwise exclusive or. In the left hand side of the diagram the output or new Xa = old Xa + Yout and new Xb = old Xb + Yout. Adding (exclusive or) the new Xa and Xb together gives the same result od adding the old Xa and Xb togther as Yout + Yout =0. Therefore if the new Xa nad Xb are introduced to the input they will yield the same Yin which with the same Zin (by a similar argument for the right hand side) must give the same Yout. When this is added to the new Xa it will yield the old Xa. The same applies to Xb, Xc and Xd.

2 (i) Euler's Totient function measures the number of elements in Zn* which is a set of all positive integers less than n which are relatively prime to n. 101 is prime so thast all numbers between 1 and 100 are relatively prime to 101. The totient function is therefore 100.

(ii) 3 is popular because only 3 exponentiations are required for encryption. The private key will be the multiplicative inverse of the public key mod totient function. Therefore for the multiplicative inverse to exist 3 must be relatively prime to the totient function on n. Thus the totient function should not be divisible by 3.

(iii) Refer to lecture handout

(iv) RSA is computationally intensive. Using a message digest to compress the message prior to signature reduces the workload. In respect of this application it should not be computationally feasible to find two messages with the same message digest and given one message and message digest it should not be computationally feasible to find another message with the same digest.

3. The main points about the proposed system are as follows.

The checksum on the magnetic stripe which is used to check the PIN is not a keyed hash. Therefore fake cards could be produced with PINs that check if the hash function is known. Since the hash function was the result of university research it would be difficult to keep secret. Improve by including a secret store key in the hash. The use of a special hash is questionable. It would be preferable to use a standard hash known to have passed the test of time.

The communications through the internet has not been secured. It would be vulnerable to interception in which transactions could be deleted or altered and the attacker would only need to recomputed the TCP checksums and final file checksum. Improve by using IPSec with ESP providing both authentication and privacy. This could be achieved by IPSec outboard devices included within the body of the ATM and in the FM centre.

Processing of the information is conducted at an FM centre. Checks should be made on the security practice at this centre including its personnel policy. The stored data can be used to make replica cards. If an FM centre must be used it would be preferable to use one which has a good record for processing financial data in a secure manner.

4(i) Refer to lecture handouts

(ii) Endpoint Identifier Hiding

(iii) The first exchange is a Diffie Hellman key exchange. An attacker cannot calculate the resulting key by observing the messages. As the messages are signed this gives protection against a bucket brigade attack. In summary it is secure against passive and active attacks.. The protocol exhibits perfect forward secrecy so that if the key and the Diffie Hellman secrets a and b are destroyed a later compromise of either end's database will not yield information by which the communication can be deciphered.

5. (i)

(a) PGP and S/MIME both employ standard algorithms – refer to lecture handouts for details
(b) PGP uses an anarchic system for key distribution and certification. Public keys may be exchanged informally and PGP users are invited to add their own contacts

to directories. A PGP user must make his own decisions in respect to the degree of trust placed in a chain of certificates. S/MIME uses a form of certificate hierarchy which although not as rigid as PEM (e.g. cross links are allowed) is normally based on organizational structure. Refer to lecture handouts for details

(c) S/MIME would be much more suitable for high value e-commerce than PGP. Non-repudiation could ve very important for many high value transactions and therefore there must be trust in public keys.

(ii) Source authentication confirms the name of the originator of the message. Non-repudiation provides the recipient with proof that the message was sent by the originator. Message integrity ensures that the message is received unaltered. Using SHA-1 to form a digest of the message followed by creating a signature of the digest using the private key of RSA could be used to provide all three functions.

(iii) Refer to lecture handouts. The "delegation of rights" feature could be used by a machine organizing an overnight production run in which another machine requires access to data in some part of the process.

6 (i)

Level 1 security can be provided by simple line encryptors
Level 2 security can be provided by protocol sensitive line encryptors
Level 3 security can be provided by IPSec
Level 4 (or more correctly interfacing on top of level 4) security can be provided by SSL
Level 7 security is provided at the application level (e.g. interfacing directly with a payment application)

(ii) Refer to lecture handouts. Transport mode is appropriate for end to end secure communications.

(iii) Refer to lecture handouts