E4.44
SO21
ISE4.45

IMPERIAL COLLEGE LONDON

DEPARTMENT OF ELECTRICAL AND ELECTRONIC ENGINEERING
EXAMINATIONS 2005

MSc and EEE/ISE PART IV: MEng and ACGI

Corrected Copy

NETWORK SECURITY

Tuesday, 10 May 10:00 am

Time allowed: 3:00 hours

There are SIX questions on this paper.

Answer FOUR questions.

All questions carry equal marks

Any special instructions for invigilators and information for candidates are on page 1.

Examiners responsible	First Marker(s) :	P.J. Beevor
	Second Marker(s) :	E. Gelenbe

Special instructions for invigilators: None

Information for candidates: None

1 (a) Explain how the RSA algorithm may be used to create digital signatures Explain why RSA digital signatures are normally used to sign a Message Digest instead of the message itself. What advantages does a digital signature created by a public cryptographic system have over a MAC created by a secret key algorithm and a shared secret?

[5]

(b) What are the advantages of using a public key exponent of 3 in the generation and verification of RSA digital signatures? In what circumstances would it be impossible to use 3 as an RSA public key exponent?

[3]

(c) In a simple demonstration of the concept of RSA digital signatures, it was decided to use either the pair of small primes 23 and 29 or 19 and 23 as p and q where the public key modulus is $n = p \: x \: q$. Show that if a public key exponent of 3 is to be used in the demonstration, then 23 and 29 must be used for the p and q.

[5]

(d) In the case where p and q are 23 and 29, and the public key exponent is 3, find the private key . In this demonstration system what would be the maximum length of message digest (in bits) that could be given a unique RSA signature?

[7]

(e) In the demonstration system described above a single octet message digest of 01100100 is signed with a single octet signature of 11010001. Verify the signature.

[5]

2 (a) What is meant by a weak key in DES? Explain the possible result of choosing a weak key. If keys are chosen at random, what is the probability of choosing a weak key?

[5]

(b) Explain how the strength of DES can be increased by the use of triple encryption. What is the effective key length of triple DES? Discuss whether a double encryption with two independently chosen 56-bit keys could be used to provide the same effective key length.

[7]

(c) Figures 2.1 and 2.2 show the even and odd rounds of IDEA. Show that the even round is its own inverse.

[5]

(d) If the first two 16-bit inputs in the odd round (i.e. X_a and X_b) are 0AC4 and F20E respectively, and the keys K_a and K_b are 1C25 and 0D2A respectively, find the associated two 16-bit outputs.

[8]

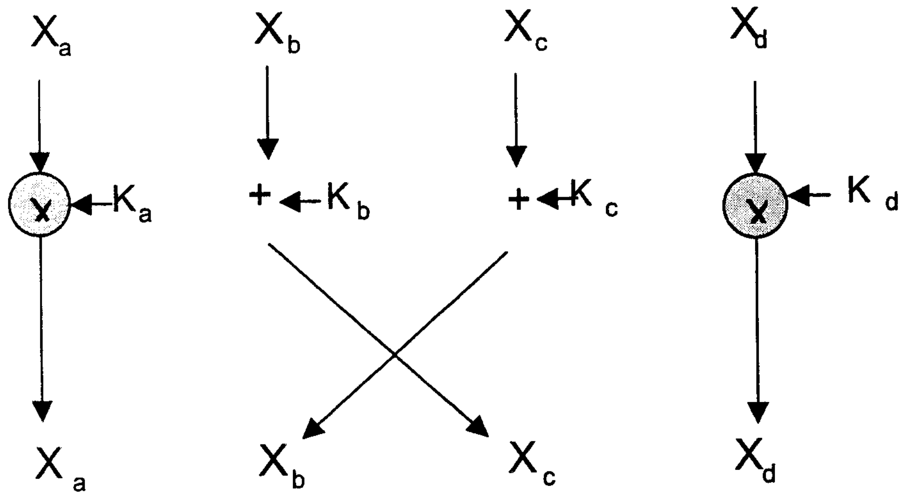


Figure 2.1 IDEA Odd Round

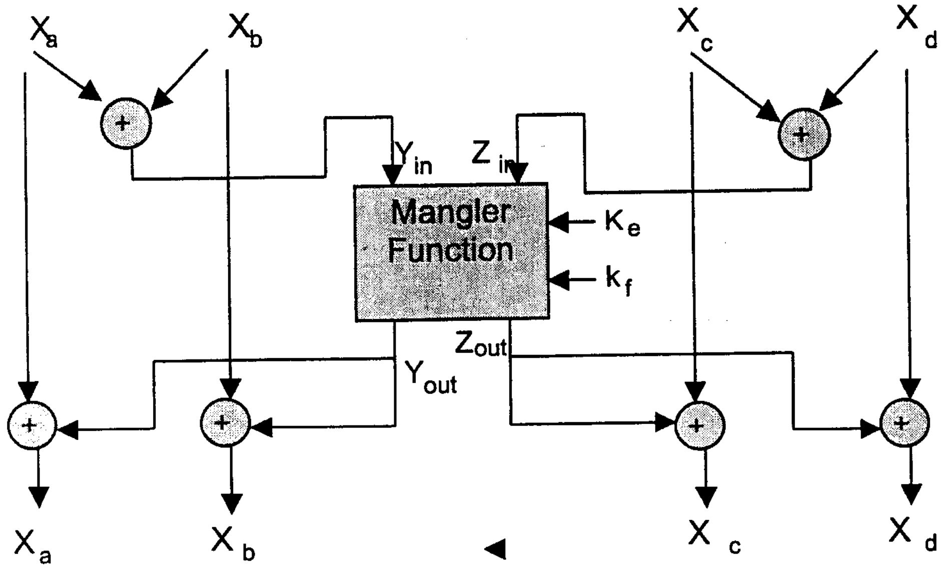


Figure 2.2 IDEA Even Round

3 (a) What are the properties of a good Message Digest function? If it were possible to find two messages which produced the same Message Digest function, explain how it might be possible to compromise a communication system which relied on that Message Digest function as part of its authentication process. In what circumstances would a Message Digest function be vulnerable to an attacker being able to find a pair of messages with identical message digests?

[6]

(b) Describe how the cipher block chaining (CBC) and the counter mode methods may be used to encrypt a stream of plaintext using a block cipher. In each case explain how decryption is performed. In what circumstances would the counter mode be preferred to CBC?

[6]

(c) What is the purpose of the initialisation vector used in CBC when the plaintext represents the following?

(i) a monthly salary statement for a company's employees;

(ii) an email message for which an individual message key is to be randomly chosen;

(iii) a standard message which is to be authenticated by a MAC created as a CBC residue.

[6]

(d) A mutual authentication system designed for a client/server relationship works in the following way. The client initiates the transaction by announcing its identity and by sending a random number as a challenge to the server. The server responds by forming a cryptographic hash of the challenge using a secret key it shares with the client. The server includes its own challenge to the client using a new randomly chosen number. The client checks the hash received and creates its own hash of the challenge using the shared secret and sends this back for the server to check. If both hashes are correct, mutual authentication has been achieved.

Analyse this authentication protocol and suggest a method by which it could be attacked.

[7]

4 (a) With reference to the OSI Reference Model, explain how security can be implemented at layers 1, 2 and 7. Give examples of systems for which security at these layers would be appropriate. [6]

(b) Figure 4.1 is an illustration of the initial handshake protocol for SSL. Explain the purpose of each line of the protocol. Explain if and how each party is authenticated. Give an example of a system for which SSL would be an appropriate security tool. [7]

(c) In the context of the IPSec protocol explain the terms *tunnel* and *transport* mode Discuss which mode would be appropriate for the following:

(i) firewall to firewall communication;

(ii) IP Virtual Private Networks. [6]

(d) Describe two ways in which the property of delegation of rights can be implemented in Kerberos V.5. Describe a possible practical application for each technique mentioned. [6]

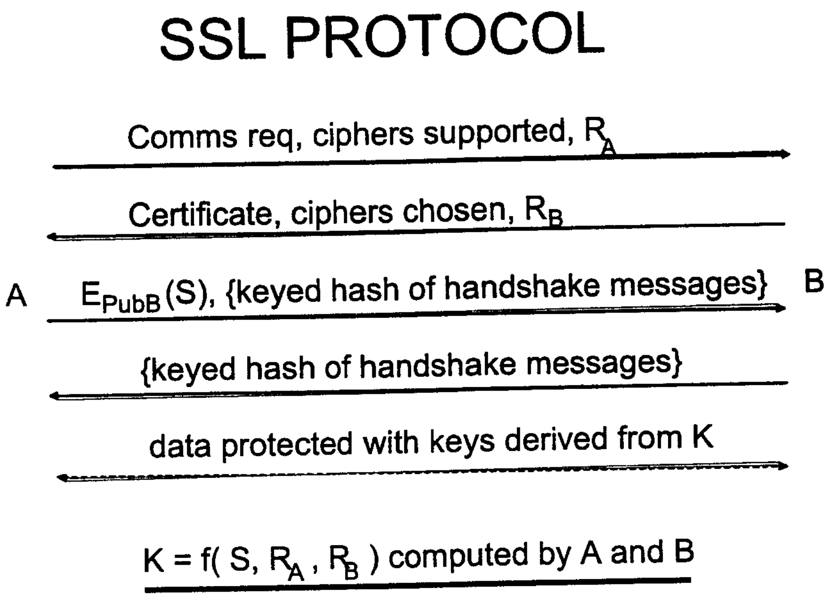

SSL PROTOCOL
Comms req, ciphers supported, R_A
Certificate, ciphers chosen, R_B
A
$E_{PubB}(S)$, {keyed hash of handshake messages}
B
{keyed hash of handshake messages}
data protected with keys derived from K
$K = f(S, R_A, R_B)$ computed by A and B

Figure 4.1

5 (a) Describe how firewalls can be configured for the following purposes:

(i) to prevent remote login from a source external to the firewall; [4]

(ii) to bar all TCP sessions initiated from outside the firewall. [4]

(b) Discuss the limitations of firewalls to provide total security. [5]

(c) The following describes a plan to provide a new internet banking service. If you were asked to conduct a security audit of the proposed operation (both the development and the operational phase) describe your approach to the task. In your discussion highlight any areas which could give rise to serious vulnerabilities

To ensure a rapid and professional development the bank has outsourced the development of its Internet banking service to an Internet Service Provider (ISP). No changes are to be made to the bank's systems for maintaining accounts, and the ISP has been asked to build a system which interfaces with the existing banking system. To assist development the ISP's software development centre has been provided with a branch banking terminal with the same facilities available to all other operational offices of the bank. This terminal is connected into the bank's live system through an Internet connection.

It is intended that, when the system is ready to go live, a section of the ISP's help desk will be responsible for registering existing bank customers onto the new internet banking service. In this connection, the ISP has been given a target to enable a customer to go live within 30 minutes of making a call to the help desk. To meet this target the ISP will ask the caller for the account name and account number/sort code, and will then effect a connection and provide the new internet customer with a login and password. At this point the new customer will have full facilities to view details on his account and to initiate new transactions. [12].

5. (a) In a public key infrastructure explain what is meant by the following:
(i) A chain of certificates,
(ii) A Certificate Revocation List,
(iii) A trust anchor.

[6]

(b) Given that the electronic mail systems PEM and PGP both use standard algorithms for authentication and encryption, explain how PEM can be considered more secure than PGP.

[5]

(c) What is meant by non-repudiation in the context of electronic mail security? Explain how it may be implemented with a public key system and with a secret key system

[6]

(d) Two parties wish to communicate by email from time to time and intend to keep the content of their communications, and the fact that communications are taking place, a total secret. Describe how they might achieve their aim.

[4]

(e) A principal wishes to send an encrypted mail to 100 recipients whose public keys are known to him. Describe an efficient way to achieve this.

[4]

Network Security 05 Answers.

Theory

1(a) Let m be message or message digest

" d be secret key exponent

" e, n be public key pair (exponent, modulus)

Then signature $S = m^d \bmod n$

Since d, e related by $de = 1 \bmod \phi(n)$

signature may be verified by forming S^e

since $S^e = m^{de} \bmod n = m^{de \bmod \phi(n)} \bmod (n) = m$

Message digest normally used to reduce computation required.

Public key signatures cannot be repudiated since can be created only by private key. Additionally signatures may be verified by any party who has the public key pair.

Theory

1(b) Use of 3 as public key exponent reduces computation required to check signatures.

If 3 is a factor of $\phi(n)$ it cannot be used since e must be relatively prime to $\phi(n)$.

Example

1(c) Let $p = 23$ $q = 29$.

$\phi(n) = 22 \times 28 = 616$

3 is relatively prime to 616 and may therefore be used.

Let $p = 19$ $q = 23$

$\phi(n) = 18 \times 22 = 396$ and 3 is a factor.

so cannot be used.

Example

1 (d) Private key may be found by using Euclid's algorithm for $e = 3$ and $\phi(n) = 616$

In this case it is simpler to note that

$de = 1 \bmod 616$

where $1 < d \leq 615$

$de = 617$ or 1233

~~1233~~ and noting that $1233 = 411 \times 3$

$d = 411$

Any message to be signed must be smaller than the modulus n

$n = p \times q = 23 \times 29 = 667$

Max bit length is ~~therefore~~ 512 bits $= 2^9$) or a 9-bit message.

($2^9 < 667 < 2^{10}$)

Example

1 (e) Message $= 01100100 = 4 + 32 + 64 = 100$

Signature $= 11010001 = 1 + 16 + 64 + 128$

$= 209$

To verify signature form $(209)^3 \bmod 667$

$= 9{,}129{,}329 \bmod 667$

$= \underline{100}$ and signature is verified.

2 (a) Theory

A weak is one of the following

~~Z~~ 56 zeros.

56 ones

28 zeros followed by 28 ones.

28 ones " " " zeros.

A weak key is its own inverse. If it used to form a pseudo random block sequence for a stream cipher the sequence will simply alternate blocks.

There are 4 weak keys.

Total size of key space = 2^{56}.

Probability of choosing a weak key = $4 / 2^{56}$

= 1 in 2^{54}

Theory.

2(b) Triple DES involves the following

$$E_{K_1} \to D_{K_2} \to E_{K_1}.$$

(ie. encrypt with K_1, decrypt with K_2 and encrypt with K_1 again)

Effective key length is 128 bits

Consider the following

$$E_{K_1} \to E_{K_2}$$

In theory such a system could be attacked if a small number of plaintext/ciphertext pairs are available

If m_1, c_1 are such a pair draw up a table of possible o/ps r formed by every key k_1 on m_1. Order r in some way. Then do reverse for the possible inputs that would have given c_1 by application of all possible keys k_2. Match the first table's o/p with second table's inputs. Repeat for other plaintext/cypher text pairs until only one match. Work involved is equivalent (on average) to less than 10 56 bit exhaustive key searches. Effective key length is therefore a lot less than 128 bits.

They

2 (c) Let X_a', X_b', X_c' and X_d' be the o/ps if X_a, X_b, X_c and X_d are inputs.

If X_a' etc are used as inputs.

$$Y_{in} = X_a' \oplus X_b' = (X_a \oplus Y_{out}) + (X_b \oplus Y_{out})$$
$$= X_a \oplus X_b$$

$\therefore$ Y_{in} is unchanged and $\therefore$ Y_{out} is unchanged.

The o/ps are

$X_a' \oplus Y_{out}$ and $X_b' \oplus Y_{out}$

But $X_a' = X_a \oplus Y_{out}$

$\therefore$ $X_a' \oplus Y_{out} = X_a$.

Similar for X_b, X_c and X_d.

Example

2(a) $X_a = 0AC4 = 4 + 12 \times 16 + 10 \times 256$ $\underline{5}$

$= 2756$

$K_a = 1C25 = 5 + 2 \times 16 + 12 \times 256 + 16 \times 256$

$= 7205$

$X_a' = X_a \times K_a \pmod{2^{16} + 1}$

$= 19,856,980 \bmod 2^{16} + 1 = 64,806$

$= 15 \times 4096 + 13 \times 256 + 2 \times 16 + 6$

$= \underline{FD26}$

$X_b = F20E$

$= 15 \times 4096 + 2 \times 256 + 14$

$= 61966$

$K_b = 0D2A = 13 \times 256 + 2 \times 16 + 10$

$= 3370$

$X_c = X_b + K_b \bmod 2^{16} = 65336$

$= 15 \times 4096 + 15 \times 256 + 3 \times 16 + 8$

$= \underline{FF38}$

2(e) ~~It would be possible to~~

Theory

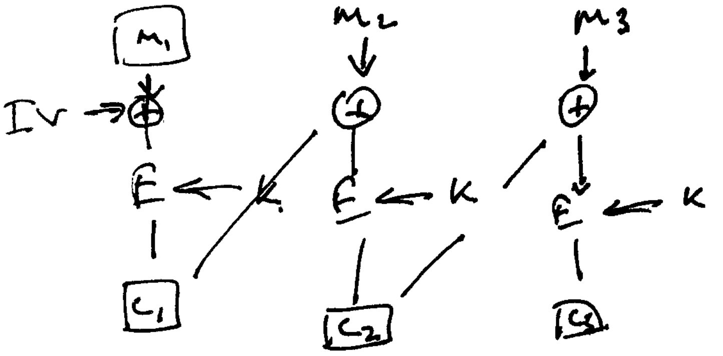
3(a) A good message digest function should have the following properties:

For a given message m and message digest MD it should be impractical to find m from MD. In addition it should be impractical to find two messages m_1 and m_2 which have the same MD. If it were possible to find two messages with same MD a signed message could be replaced by another without invalidating signature.

If the MD is too short then it might be possible through the Birthday Paradox to find two messages with same MD. For example for a 64 bit MD it would be necessary to check out 2^{32} possible messages to find a match.

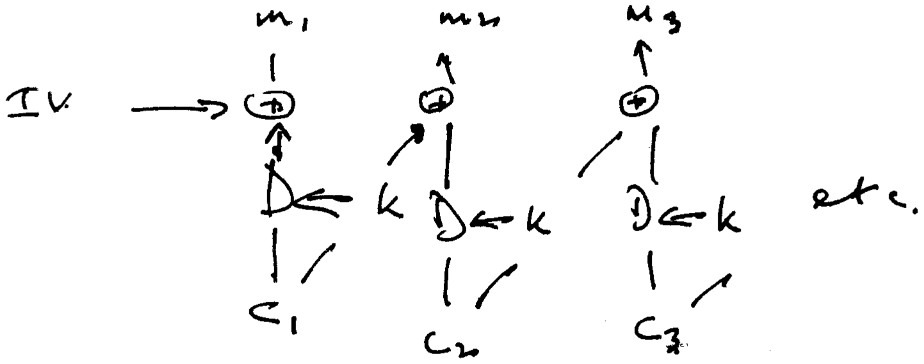
3(b) Theory

CBC works as shown below.

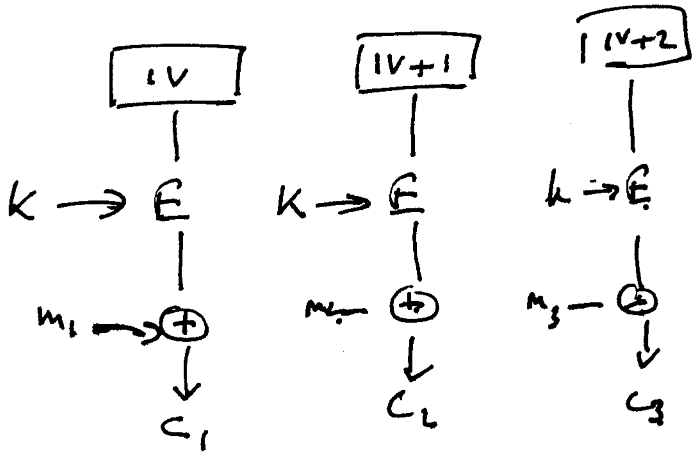


etc

Decryption as below (CBC)



Counter Mode as shown below.



For decryption in counter mode simply interchange c_i and m_i

Counter Mode would be preferable for a look-up table.

Example

3(c) The IV has the following uses

(i) If the same key is used to encrypt the salary statement every month then without an IV any change in salaries will be immediately apparent

(ii) An email message typically starts in a standard way (e.g. Dear Sir or Hi etc). An exhaustive key search becomes easier if the lack of a standard greeting is apparent.

(iii) If the key is not changed the MAC would be predictable for a standard message.

Example

3(a). The protocol is illustrated below

A $\xrightarrow{I'm\ A,\ R_A}$

$\xleftarrow{H_k(R_A),\ R_B}$

$\xrightarrow{H_k(R_B)}$

This protocol is vulnerable to a replay attack. A would start a session and when challenged with R_B open up a new session using R_B as its own challenge. When B replies with $H_k(R_B)$ A can complete the first session and abandon the second.

4(a) Theory / application

Layer 1 is physical layer. A simple line encryptor would provide security at this layer.

Layer 2 is ~~protocol lo~~ link data layer. A protocol sensitive line encryptor provides security at this layer.

Layer 7 is the application layer. Adding security to specific transactions in an application program is effective security at this layer.

Layer 1 may be used effectively to provide privacy on a point to point telecommunication link (eg the line from a bank outlet to a processing centre). ~~Layer~~ 2 may be used for an X.25 or FR ~~closed~~ virtual private network. Layer 7 is best used for complex transactions (e.g. payment authentication in banking).

4 (b) Theory

Line 1 A asks for communication and offers ciphers which it supports. A also transmits random number R_A which will be used later to form a key.

Line 2 B sends A its certificate which contains B's public key. B informs A the ciphers it has chosen and its own random number R_B.

Line 3 A chooses pre-master secret S and sends this encrypted under B's ~~master~~ public key

A also sends a hash of the master secret K and a hash of the handshake messages. This proves A knows key and that handshake messages have not been altered.

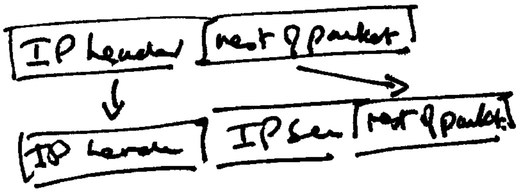
Line 4 B proves by the hash that it knows the key K and that all handshake messages are unaltered. This also proves B knows its own private key which would have enabled it to find S.

In the following A has authenticated B but ~~A has~~ B has not authenticated A.

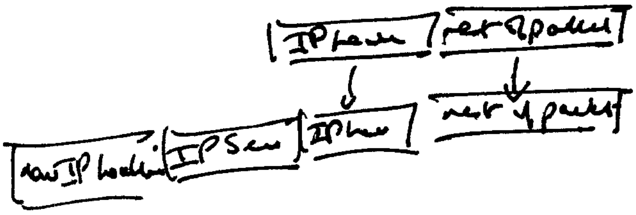
SSL is appropriate for most web browsers.

4(c). Theory

In transport mode IPSec information is inserted into the packet as shown below



By contrast in tunnel mode a new IP header is added for the tunnel



For firewall to firewall communication a tunnel
would be built between the firewalls. Either
mode could be used to IP VPNs.

Theory.
4(a) Two ways for delegating rights are by
'forwardable' and 'proxiable' TGTs. A
'forwardable' TGT may be exchanged for a TGT
with another network address. In the case of
a 'proxiable' TGT it may be used to request tickets
for use by another network address.
A might wish B to provide some
As ~~examples~~
batch task overnight. In the forwardable case
B has a TGT for A which it exchanges for a
ticket. In the proxiable case A provides B with
the ticket it needs.

Example
5 (a) A packet filter may be set up in a
firewall to bar any activities considered undesirable
A packet filter examines the protocol field in
the IP header and may deduce for example if
(i) a remote login is being attempted. The filter
spots the source address is outside the wall and that
the protocol field / TCP port specifies remote login
and the communication is barred. In the case of
barring all TCP sessions initiated from

out side the firewall the packet filter must examine the TCP header for a ACK flag. If it is not there and the source address is outside the wall then it follows a session is being initiated from outside and will be barred.

Theory.

5 (b) Firewalls can be effective in barring certain types of communications as discussed above. However they are defenceless against any compromise of machines inside their wall of protection.

Application

5 (c) The main points that should cause concern in a security audit are as follows.

Development Phase.

- development should not be undertaken on a live system - a development machine should be used.
- the software developers are outside the control of the bank - there needs to be some HR/security checks and regular audit to prevent trapdoors being built into programs.
- the siting of a live bank terminal in the ISP's premises is a huge risk to fraud.
- although it is not the principal threat the communications through the Internet should be protected by for example IP Sec.

Operations Phase

- There is little ~~control~~ authentication of customers who ~~and~~ seek connection to the server. ~~It is~~ Anyone may obtain account details without any authorisation to use an account. Application should be in writing and any passwords should be posted to the account holder at his normal address. Logins should be sent under separate cover.

- There needs to be HR/security controls on help desk staff who could perpetrate fraud

- There is no mention of changing passwords or of any repeat authentication.

- Even with good authentication at registration and with all transactions some limit must be placed on transactions (eg. decline same day value).

6. (a) Theory

(i) A chain of certificates allows a distant party to be verified by intermediaries in the chain. Eg if A signs B's certificate and C signs A's certificate, D signs C's certificate etc then the chain to B is through D and C and A.

(ii) A Certificate Revocation List is a published list of all certificates revoked at a particular time.

(iii) A trust anchor is an entity whose public key is known and trusted in advance.

Theory

6 (b) Although PGP makes use of much the same algorithms as PEM the familiar parts of a public key infrastructure, namely trust anchors, certificates, certificate revocation lists are lacking. PGP is follows the anarchy model for a PKI and the user must to a certain extent take public keys at face value. By contrast PEM has a strict Certificate Hierarchy in which CAs are classified according to security level exhibiting and may be trusted to certify others of the same security level. In that sense PEM is a more secure system.

Theory.

6(c) Non repudiation in an electronic mail system is the property which prevents the sender from denying he sent the message.

In a public key system the property follows from the use of digital signatures which can be created only by the holder of the private key. In a secret key system a third party or notary is required to provide non-repudiation

A sends an authenticated message to the notary using the secret shared with the Notary. The Notary checks the authenticator and using his own secret creates a seal (a cryptographic hash) of the message and A's name which it appends to the message. The message is sent to B authenticated by N and carrying N's seal which can be used later to prove A sent the message.

Example

6(a) A and B should encrypt their communications and send through a third party who must additionally send out a large number of dummy messages. The dummy messages obscure the fact that A and B are communicating through the third party.

6(e) Example

The principal should choose a session key at random and encrypt the message using some standard secret key algorithm such as DES or IDEA. He should then encrypt the session key with each of the recipients' public key and attach the individually encrypted session key to each copy of the message sent.