E4.44
SO21
ISE4.45

IMPERIAL COLLEGE LONDON

DEPARTMENT OF ELECTRICAL AND ELECTRONIC ENGINEERING
EXAMINATIONS 2007

MSc and EEE/ISE PART IV: MEng and ACGI

NETWORK SECURITY

Monday, 14 May 10:00 am

Time allowed: 3:00 hours

Corrected Copy

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

Special instructions for students

None

The Questions

1. a) Figures 1.1 and 1.2 show respectively the odd and even encryption rounds of the IDEA algorithm. Explain how decryption can be achieved in each case, justifying your answer with appropriate supporting analysis. [5]

b) If the keys K_a, K_b, K_e and K_f in Figures 1.1 and 1.2 are respectively *0A24, B2C7, 5C89* and *289D* determine the relative keys required for decryption. [7]

c) Figure 1.3 shows the *MixColumn* operation of an AES encryption round. Explain the process shown in Figure 1.3, stating whether the operation should be considered a permutation or substitution in the block cipher. Explain further how the relative decryption operation can be achieved, justifying your explanation with appropriate analysis. [6]

d) In an operation with the AES cipher it is required to find the inverse polynomial of $x^4 + 1$ modulo $x^8 + x^4 + x^3 + x + 1$, both polynomials being over Z_2. Explain how Euclid's algorithm can be used to find the inverse polynomial of $x^4 + 1$, illustrating your answer by completing the first two calculated rows of Euclid's algorithm (you are not required to find the inverse polynomial). How would this operation be achieved in a practical implementation of AES? [7]

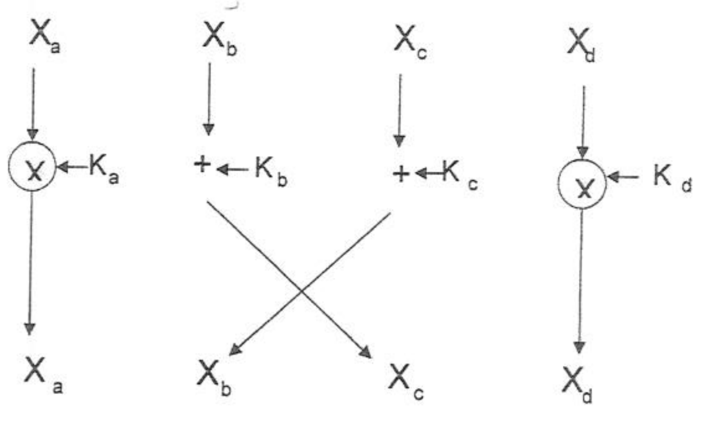

Figure 1.1 IDEA Odd Round

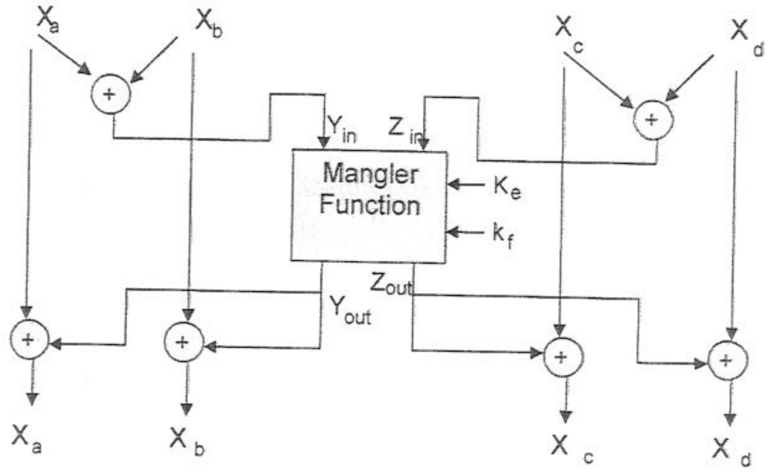

Figure 1.2 IDEA Even Round

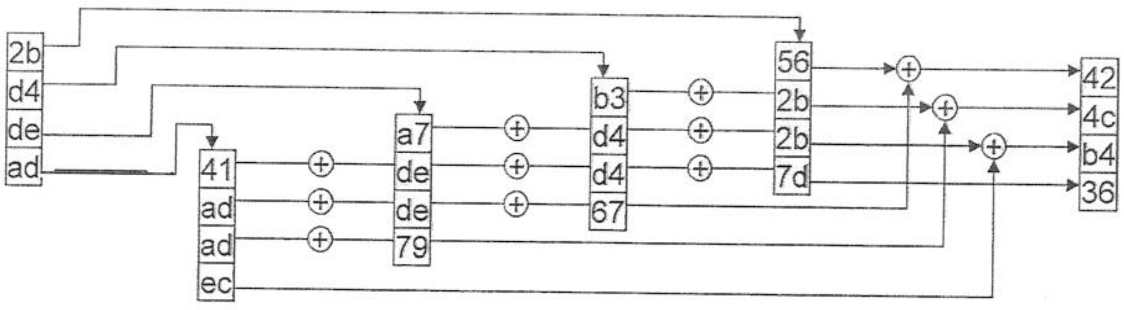

Figure 1.3 Mix Column Operation in AES

2. a) In the RSA system of public key cryptography, a principal with another's public key pair (e, n) encrypts a plaintext message m to form the ciphertext $c = m^e \, mod \, n$.

i) Explain in detail how the intended recipient of the message may use his private key to recreate the message m. [4]

ii) Explain how an attacker provided with unrestricted computing resources could retrieve the plaintext. [4]

iii) What restrictions must be placed on the length of the message m to ensure that it can be unambiguously deciphered? [2]

iv) If the message m is one of a limited number of standard messages that may be sent, what would be the most efficient method for the attacker to decipher the plaintext? [3]

b) The triple DES (3DES) system of cryptography uses 3 standard DES operations (encrypt – decrypt – encrypt or EDE) to convert plaintext into ciphertext.

i) What is the standard message block size used in 3DES? [2]

ii) What is the effective key length of a 3DES system? [2]

iii) What are the advantages of using the DES operations EDE over other possible combinations of 3 standard DES operations? [3]

iv) If only two standard DES encrypt operations (EE) are used to increase the effective key length of DES, what method of attack may be used to ensure that the intended increase in key length is not achieved? [5]

3. a) Discuss what properties should be present in a good message digest function. Suggest two applications of such a function, and explain in each case why these properties are essential. [6]

b) In the context of message digest functions, explain what is meant by the 'birthday paradox'. What are the implications of the 'birthday paradox' for the length of the message digests currently in use? [5]

c) Figure 3.1 shows the outline design of the message authentication code known as HMAC which uses 'Secure Hash Algorith-1' (SHA-1). Explain why the design uses two separate paths to form the final message authentication code. [7]

d) In order to reduce the complexity of HMAC a simpler design is proposed. In this design the message is divided into 160-bit blocks and each block forms one input into a stage of the digest for which the other input is the 160-bit output of the previous stage. In each stage of the digest the current 160-bit message block is rotated 32 bits to the left and added modulo-2 to the output of the previous stage. The result is the output of that stage.

Discuss whether this design would exhibit the properties of a good message digest function, and, if not, propose a method by which such a system could be attacked. [7]

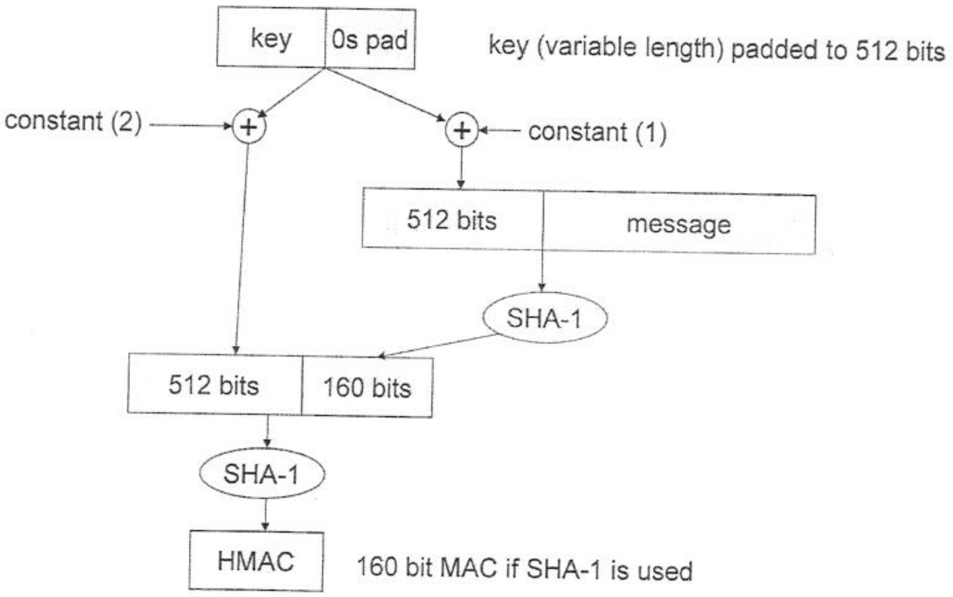

Figure 3.1 Outline Design of HMAC

4. a) What is the function of the Key Distribution Centre (KDC) in the Kerberos system of network security? What feature of the design of the KDC is intended to ensure high availability? How is secure communication achieved between two principals which are not connected to the same KDC? [5]

b) Describe three differences between Kerberos V4 and Kerberos V5. What features of V5 not present in V4 should be of interest to an IT manager of a major business? [5]

c) Explain what is meant by 'Perfect Forward Secrecy' (PFS) and describe one method by which it may be achieved. Does Kerberos (V4 or V5) exhibit PFS? [5]

d) In the context of the 7-layer OSI Reference Model of communications describe how security may be established at layers 1, 2, 3, 4 and 7 and describe briefly the issues involved with layers 1, 2, and 7. [5]

e) If secure communication is required between two principals connected to the same IP network, and the security systems available are IPSec and TLS, discuss the security requirements that would make IPSec the chosen option. [5]

5. a) Two principals which share a secret one-time pad are connected through an optical fibre link. Explain how quantum cryptography can be used to establish totally secure communication between the principals. Explain further how quantum cryptography can be used to establish the shared secret one-time pad without the use of any techniques from conventional cryptography. [10]

b) A government wishes to issue identify cards to its citizens using smart card technology with the data secured by conventional cryptography. In order to make use of local knowledge to confirm an individual's identity, a large number of reception centres are set up in local government offices. The applicant is interviewed in the reception centre, and biometric and other personal data is collected. This data is sent through the internet to a central government office and is protected through the internet by means of an IPSec VPN. The central office sends the data to a specialist contractor (part of a multi-national group) together with a 512-bit government RSA key which is intended to be used to create a signature on the personal data. The contractor is responsible for producing the identity cards, which may be checked for validity by comparing the biometric data in the card with that exhibited by the cardholder, and by verifying the government signature on the personal data.

The government wishes to recover the cost of developing and manufacturing the identity cards with a high charge to its citizens, and, to aid its introduction, the government guarantees a card lifetime of 20 years.

You are a security consultant invited by the government to audit the proposed scheme. What would be your major concerns about security, and what additional information would you require to undertake an effective audit? [15]

6. a) Explain how a firewall, placed between a corporate LAN and the internet, can be configured to provide the following protection:

i) allow all communications except that using the TELNET protocol;

ii) allow all file transfer communications initiated from within the LAN but block all similar communications initiated from outside the LAN. [5]

b) What is meant by a 'denial of service attack'? What techniques are available to protect vulnerable servers on the internet from such attacks? [5]

c) What features should be exhibited by a good public key infrastructure (PKI)? Describe in outline the PKIs employed by 'Privacy Enhanced Mail' and 'Pretty Good Privacy'. [5]

d) Explain what is meant by a 'replay' attack and provide an example where such an attack would be possible. Explain further how a modification to your example would serve as protection against such an attack. [5]

e) i) In the context of email security explain what is meant by 'non-repudiation'. Explain further why the property of non-repudiation is important in e-commerce applications. [2]

ii) One party on an email system wishes to send securely the same email to 100 recipients on the same email system. All parties to the communication are provided with standard systems of secret (e.g. DES, IDEA, etc.) and public (e.g. RSA) key cryptography. Propose an efficient way for the broadcast email to be sent. [3]

Network Security 2007 Answers.

1 (a)

For the Odd Round.

$$X_a' = X_a \times K_a.$$

$$\therefore X_a = X_a' \times K_a^{-1}$$

Decryption uses same structure with multplicatin ~~mode~~ inverse key K_a^{-1} (mod $2^{16}+1$)

$$X_b' = X_c + K_c$$

$\therefore X_c = X_b' + K_c'$ where $K_c + K_c' = 0$
ie K_c' is additive inverse of K_c mod 2^{16}

Decryption uses same structure with additive inverse key.

③

Similarly for X_b and X_d.

For the Even Round

$$\begin{aligned} X_a' &= X_a \oplus Y_{out} \\ &= X_a \oplus M(Y_{in}) \\ &= X_a \oplus M(X_a \oplus X_b) \end{aligned}$$

but $X_a' \oplus X_b' = X_a \oplus X_b \oplus Y_{out} \oplus Y_{out} = X_a \oplus X_b$

$$\therefore X_a = X_a' \oplus M(X_a' + X_b')$$

②

Decryption uses same structure and same keys.

1 (b). k_e' and k_f' are the same as k_e and k_f

$k_e' = 5C89$

$k_f' = 289D$ 1

k_b' is additive inverse of k_b

~~k_b' =~~ ~~3AAD~~ k_b = B2C7

(~~k 3AAD~~ +

$k_b' + B2C7 = 0 \mod 2^{16}$

$k_b' = 4D39$ ~~2~~ 1

$k_a' = k_a^{-1}$

Use Euclid's algorithm for numbers $2^{16}+1$ and k_a

k_a = 0A24 = 2596 decimal

$2^{16}+1$ = 65,537 decimal

n	q	r	u_n	v_n
−2		65537	1	0
−1		2,596	0	1
0	25	637	1	−25
1	4	48	−4	101
2	13	13	53	−1338
3	3	9	−163	4115
4	1	4	216	−5453
5	2	1	−595	+15021

∴ k_a^{-1} = 15021 decimal = 3~~BE~~D
AA

5

1(c)

The input is a 4-octet column vector. Each octet is replaced by a new octet and placed at the top of each of the four intermediate column vectors. Bit wise mod 2 addition is used to form the output 4-octet column vector.

The process involves substitution of each octet in the input column and so must be considered a substitution process. ~~4/2~~ 3

As bit-wise mod 2 addition is easily reversible ($a \oplus b = c$, $\therefore a = b \oplus c$) it is a simple matter to derive an inverse look up table to reverse the process 3

1 (d).

The polynomial $x^8+x^4+x^3+x+1$ is irreducible so that it must be relatively prime to x^4+1. Using these two polynomials as in Euclid's algorithm will therefore leave a final remainder of 1

This final row may be used to find the inverse polynomi of x^4+1 in a similar way to that used for the inverse key in 1(b). 3

The first two calculated rows are shown below

n	q	r	u_n	v_n
-2		$x^8+x^4+x^3+x+1$	1	0
-1		x^4+1	0	1
0	x^4	x^3+x+1	1	x^4
1	x	x^2+x+1	x	x^5+1

In a practical implementation of AES a look-up table would be used for the inverse polynomials 4

2 (a)

(i) $c = m^e \bmod n$

Recipient has private key d where
$de = 1 \bmod \phi(n)$

Recipient takes c and forms $c^d \bmod n$

but $c^{ed} \bmod n = m^{de} \bmod n = m^{de \bmod \phi(n)} \bmod n$

$= m \bmod n = m$ ~~since m~~ 4

(ii) An attacker needs to find d from the information $de = 1 \bmod \phi(n)$

He knows $n = p \times q$ where p, q are prime and therefore $\phi(n) = (p-1)(q-1)$. Therefore, if the attacker can factorise n into p and q, he will have $\phi(n)$ and he may calculate d from Euclid's algorithm as the multiplicative inverse of e $\bmod \phi(n)$. 4

(iii) m must be of length less than n bits so that $m = m \bmod n$ 2

(iv) The attacker should form the ciphertext for each known plaintext by calculating $c = m^e \bmod n$ and then compare the sender's ciphertext with his table of ciphertext. 3

2(b)

2 (i) The standard block size is 64 bits (as in DES)

(~~ii~~

2 (ii) The effective key length is 112 bits

(iii) The 3-DES standard is

$$E_{k_1} - D_{k_2} - E_{k_1}$$

If D_{k_2} were replaced by E_{k_2} the final permutation of E_{k_1} would be reversed by the first permutation of k_2. In addition if $k_1 = k_2$ the standard 3-DES reverts
3 to standard DES which it would not if the second operation were an E or the first and third operations were D_s.

(iv) If $E_{k_1} - E_{k_2}$ were used to give an apparent key length of 112 bits, the following attack would be possible.

A known plaintext / ciphertext pair should be selected and a large table formed with all possible keys (2^{56}) to find the intermediate ciphertext from the E_{k_1} operation and the intermediate 'plaintext' from the E_{k_2} operation (which gives the resulting known ciphertext). There will be a number of matches for the intermediate ciphertext and plain text. These should be tested against another known plaintext / ciphertext pair and the process repeated until after a few
5 stages only one k_1 and k_2 will be found to be a match for all trial plaintext/ciphertext pairs.

3

(a)

For a good message digest function it showed not be ~~possible to~~ feasible to find a message which has the same message digest as another specified message. Furthermore it showed be infeasible to find two messages with identical message digests. 2

One application of a message digest is to form a message authentication code (MAC) of a message by concatenating a secret key k with a message and calculating the message digest of the key and message. A second application is in the creation of a digital signature to a message. In this second application a digest is created from the original message, and the digest is then signed. 2

In each of these applications the first property of a good message digest function prevents the real message being substituted by a false message leaving the MAC or signature unchanged. The second property prevents a fraudster from preparing pairs of messages of which one will be authorised and another sent. 2

(b) The 'birthday paradox' ~~is the~~ refers to the surprisingly high probability that two messages may be found with the same message digest for a particular message digest function. 2

If there are n people in a room and k (= 365) possible birthdays then prob that two people are found with same birthday

is approximately $\frac{n(n-1)}{2k}$. For this to reach a probability of 0.5 or more $n \geq \sqrt{k}$.
~~In the~~ For a message digest ~~case~~ of length L bits $k = 2^L$ and n is the number of trials.

3 To find two messages with the same digest we would expect to test $2^{L/2}$ messages. 2^{64} tests is considered infeasible and therefore L should be at least 128 bits.

(c) In a simple MAC design based on a standard message digest function, the secret key k is concatenated with the message at the beginning of the message and each block of message (typically 512 bits) is processed ~~with the output of~~ in its stage with the output of the previous stage. ~~Knowin~~
7 The message digest function which is used in each stage it would be possible to add another block to the message and calculate the correct MAC. In the HMAC design this would not be possible.

(d) This design would not exhibit the properties of a good message digest function as it would be relatively easy to find a
7 number of messages which would have the same message digest as a specified message. An attacker would simply change each 160 bit block so that the final mod-2 addition would remain unaltered.

4

(a) The KDC is effectively the security
management centre ~~of~~ in a Kerberos
implementation. It is responsible for validating
2 the identity of principals connected to the
system and of providing session keys for
secure communication between two principals.

An important feature of the KDC as regards
overall availability of the system is the largely
2 static database. It achieves this by providing
information in ticket granting tickets which is
held by the principals and not by the KDC.

If two principals are not connected to the same
KDC secure communications may still be achieved
by KDC-KDC secure communications. In V4 each KDC
1 must be connected directly to every other KDC
of interest whilst in V5 the KDCs may be
networked to achieve the same result.

(b) A possible selection of 3 differences between
V4 and V5 are (other combinations are possible):

- V5 allows networked KDCs (ie each KDC does not require a direct connection to every other KDC of interest);

3 ~~–~~

- V5 uses international standards in syntax and naming conventions;

- V5 allows delegation of rights from one principal to another.

All three of above should be of interest to
an IT manager. The first allows greater flexibility
in secure external communications. The second ~~support~~
2 minimises IT support costs and the third allows
the creation of a security manager to control
the entire IT operation.

(c) Perfect Forward Secrecy ~~also~~ is a feature
which allows an attacker to record all
protected communications between two principals
2 without compromising ~~the system if the~~ if the
attacker later gains access to one or both of
the principals involved.

One method of providing PFS is to create
session keys using Diffie Hellman and then
2 to 'forget' the session keys and the original
Diffie-Hellman secrets immediately at the end
of each session.

1 Kerberos does not exhibit PFS because it
holds ~~master to~~ information on master keys for
the principals.

(d) Layer 1 security may be provided by standard line encryptors with a pair of encryptors protecting each circuit between two nodes of a network.

Layer 2 security may be provided by protocol sensitive line encryptors which leave Layer 2 protocol information in clear.

Layer 3 security may be provided by IPSec in an IP network.

Layer 4 security may be provided by TLS in an IP network

3 Layer 7 security may be provided in any network by building in security ~~at~~ within ~~o~~ the application (e.g ~~seco~~ banking security within payment messages independent of communications employed)

The main issue with Layer 1 security is that all information is in clear at the network nodes

Layer 2 security closes the above loophole at the expense of complexity and hence reliability. In addition systems are vulnerable to application level attacks at the endpoints.

2 Layer 7 security protects the application but affords no protection to information on traffic flow.

(e) TLS is most suitable for client/server communications in which the server must authenticate the client but the client does not need to authenticate the server. TLS is relatively simple and reliable and may be easily employed.

5 IPSec is more complex and requires more work in setting up a reliable connection. However it offers mutual authentication.

12

5

(a) Transmission of a message between two principals using quantum cryptography involves two transmission schemes and a shared one-time pad to indicate which transmission scheme is being used. The two schemes are rectilinear and diagonal polarisation of photons which may be represented as ↔↕ and ⤡⤢ respectively. If the receiver knows the transmission scheme used by the transmitter, he will detect the photon with an appropriate filter (rectilinear or diagonal) and measure the polarisation of the photon with certainty; if he ~~must~~ guess the ~~polaris~~ transmission scheme (as would be the case for an intercepting attacker) he will measure the polarisations correctly 50% of the time and receive no information. 5

To establish a one-time pad ~~to~~ without the use of conventional cryptographic techniques, the transmitter sends a random ~~stre~~ message with a randomly selected transmission scheme. The receiver guesses the transmission scheme and will therefore be in error 50% of the time. The transmitter then tells the receiver the transmission scheme and the receiver discards all but correct guesses (this communication is on an open line) The correctly received data is then used as the one-time pad. A sample of this is used for testing and if correct the remaining digits form the shared one-time pad. If the test fails, this indicates an attack has taken place and the process is repeated. The system works because an attacker will not guess transmission schemes in the same way as the receiver and so cannot use the information on the open line. 5

(13)

(b)

Concerns would include

- security at local reception centres – e.g can a false name (or multiple names) be attached to a valid set of biometric data?

- ~~what~~ how is the data secured between the central government office and the contractor (in particular the 512-bit key).

- contractor's personnel on site – what control does the government have over these? – are they its own citizens who may be vetted

- security of government data on contractor's site – can the key be revealed to contractor's staff or is it securely housed in a tamper-resistant module?

(15)

- lifetime of cards is at 20 years far too long for a 512-bit key → 5 years would be more appropriate with a 2048 bit key.

14

6

(a)

(i) The firewall should be configured to
2 examine the protocol code at level 4 and should
exclude all packets bearing the TELNET code

(ii) The firewall should look for the ACK
response in the TCP packets. If this appears
3 in incoming packets from the Internet the
session should be allowed. If, however, it appears
in outgoing packets the session should be blocked.

(b) A 'denial of service' attack is where a
2 server ~~is~~ receives a huge number of service
requests so that congestion occurs and legitimate
~~3~~ requests are blocked. All techniques involve an
immediate reply to all requests which may just
test the authenticity of the sender's address or
3 may request ~~tasks~~ time consuming tasks of the sender
which are easy to check at the receiver.

(c) A good PKI should exhibit the ability to
- issue certificates
3 - revoke certificates previously issued
- authenticate certificates

Privacy Enhanced Mail (PEM) uses a highly
structured system involving 3 levels of trust /
security. All certification authorities (CAs) must belong
1 to one of these 3 groups (high security, medium
security and low security) and may only communicate
with others in the same group.

Pretty Good Privacy does not really have a PKI in
that any principal may act as a CA and issue
certificates which may or may not be trusted by
1 others. This imposes more work on each principal
to evaluate the trust that may be placed in
any certificate received.

(d) A 'replay attack' is one where an attacker
records information sent in a legitimate
communication and re-uses it to gain
unauthorised access to a system. Alternatively
2 the attacker may induce the respondent to
divulge information which may be re-used in a
later session.

An example of the latter is in challenge/
response type of authentication. An attacker may
issue a challenge and obtain a correct response
and his own challenge to which he cannot respond.
3 He then ~~breaks the session~~ opens a new session
with the very challenge he himself received. Having
received a correct response he may complete the
first session successfully.

(e)(i) Non-repudiation is the property which prevents
a sender of information denying later that he
sent the specified communication. It is very
2 important in trading applications where prices
may change rapidly.

(ii) A randomly chosen key should be used to
3 encrypt the message. This key should be sent
to every recipient encrypted under the recipients
public RSA key.