E4.44
SO21
ISE4.45

IMPERIAL COLLEGE LONDON

DEPARTMENT OF ELECTRICAL AND ELECTRONIC ENGINEERING
EXAMINATIONS 2006

MSc and EEE/ISE PART IV: MEng and ACGI

NETWORK SECURITY

Wednesday, 17 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) A DES encryption round is illustrated in Figure 1.1. Explain, with reference to a similar diagram, how decryption is achieved in a DES round.

[5]

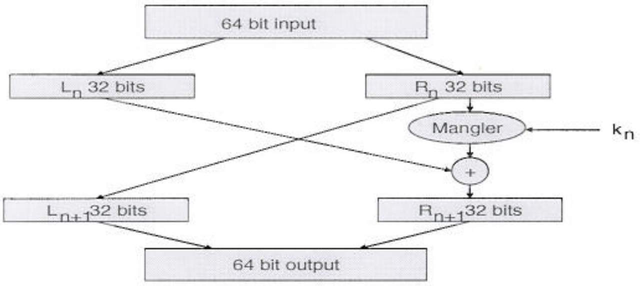


Figure 1.1 A DES round for encryption

(b) The generation of per-round keys is illustrated in Figure 1.2. . By reference to this diagram, explain what is meant by a weak key and define all weak keys. Show that a weak key is its own inverse (two keys are inverses if encryption with one is the same as decryption with the other)

[5]

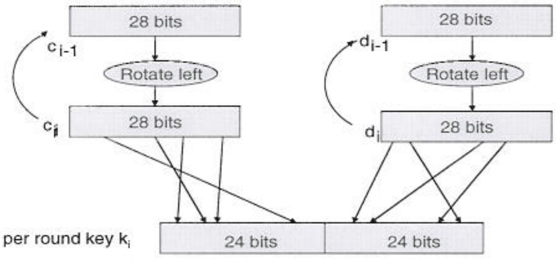


Figure 1.2 Generation of the per-round keys in DES

Question 1 is continued on the next page

(c) A message is required to be communicated securely between two parties who share a secret in the form of a 56 bit DES key. The following methods for encryption are proposed:

(i) DES

(ii) 3DES with the first key as the shared secret and the second key a 6-bit left rotation of the first

(iii) IDEA in which the DES key (as a 64-bit key including its parity bits) is repeated to make a 128 bit key

(iv) AES-128 in which the DES key (as a 64-bit key including its parity bits) is repeated with a 6-bit right rotation to make a 128-bit key.

If the computing power required for a single encryption of a standard message in DES, IDEA and AES-128 is given as C_D, C_I and C_A respectively, compare the strengths of the four systems proposed. In your analysis assume that an attacker has knowledge of the systems proposed but not the key itself.

[5]

(d) The S-Box in AES transforms an octet represented by x^3+1 (a polynomial over Z_2) into another octet. The first operation transforms the octet into its inverse modulus $x^8+x^4+x^3+x+1$. Show that the inverse is $x^6+x^3+x^2+x+1$. If the second operation involves multiplication by $x^4+x^3+x^2+x+1$ modulus x^8+1 find the result of the second operation.

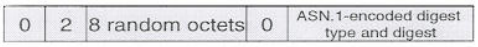
[10]

2 (a) In the RSA system of public key cryptography what should determine the length of key and the maximum length of an individual message block? If a key length of 512 bits is chosen and the message is 400 bits long, what will be the length of the resulting ciphertext block?

[5]

(b) Figure 2.1 illustrates the form of the public key cryptography standard in which the individual blocks represent octets. In the figure the second octet has value 2 which denotes encryption. Explain the purpose of the next 8 octets which are non-zero octets chosen at random.

[6]



0	2	8 random octets	0	ASN.1-encoded digest type and digest

Figure 2.1 Public Key Cryptography Standard

Question 2 is continued on the next page

(c) Figure 2.2 illustrates the nature of a Diffie-Hellman key exchange between parties A and B. Explain how such a system may be categorised as a public key system and identify the public and private keys. Explain how an attacker observing the exchange in full would be unable to ascertain the resulting shared key. Describe how the system may be compromised by an active attack and explain what measures could be taken to prevent such an attack.

[6]

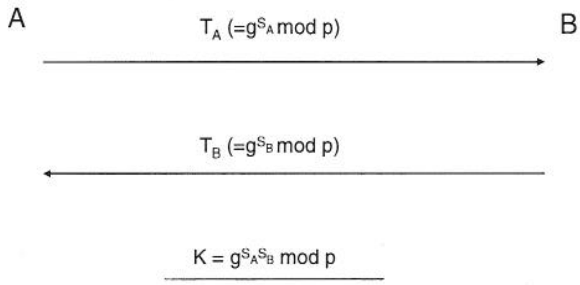


Figure 2.2 Diffie-Hellman Key Exchange

(d) A signature in the Digital Signature Standard is formed by calculating the quantity $X=S_m^{-1}(d_m+ST_m)\ mod\ q$ where S is the long term secret, S_m is the per-message secret, T_m is the per-message public key and d_m is the message digest. If the per-message secret S_m is exposed show how the long term secret S may be calculated from the signature. Show also how the per message secret may be calculated if the same per message secret is used to compute the signature on two separate messages. (hint: compare the two signatures)

[8]

3. (a) Figure 3.1 illustrates the protocol used in the Phase 1 Internet Key Exchange (IKE). In the context of IKE explain what is meant by "endpoint identifier hiding". Describe the method used in Phase 1 IKE to implement the last two lines of the protocol.

[6]

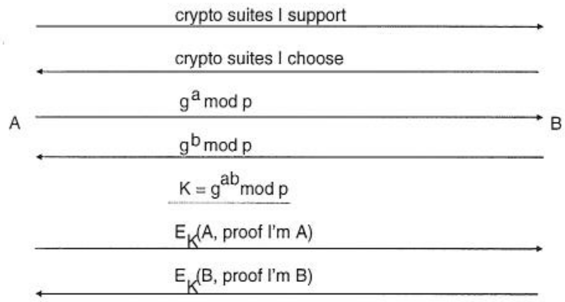


Figure 3.1 Phase 1 Internet Key Exchange

(b) In the context of IPsec protocols explain what is meant by Encapsulating Security Payload (ESP) and Authentication Header (AH). In view of the fact that ESP supports both encryption and authentication what possible advantages does AH have over ESP? Explain what is meant by tunnel mode in IPsec and give an example of where it might be useful

[6]

Question 3 is continued on the next page

(c) A firewall is placed at the gateway between a corporate LAN and the internet. Explain in outline how the firewall could be configured to provide the following functions:

(i) to bar all communications to or from a particular external address on the internet;

(ii) to bar all incoming TELNET sessions;

(iii) to bar any external machine on the internet from initiating a connection to a machine on the corporate LAN.

[6]

(d) In web security HTTP Digest Authentication is said to be a low budget security alternative to SSL. Justify this statement. Explain how the HTTP digest offers protection against a replay attack and against disclosure of the server database.

[7]

4. (a) In the context of determining a safe length for as message digest, explain what is meant by the "birthday paradox". State what you consider to be a safe length for a good message digest function and determine for such a function what would be the probability that two message chosen at random have the same message digest.

[4]

(b) A company decides to allow electronic voting at all general meetings. Each shareholder is given an ID which is his number on the share register and a password which is a hash of this ID and his address details. Passwords are included with official notices of meetings which are sent to shareholders through the post. A special web site is created to accept votes up the time of the meeting. When a shareholder connects to the site he is asked for his ID and password and if a correct ID/password pair is provided another screen appears through which voting may take place.

As the company's auditor you are responsible for ensuring that meetings are conducted properly. In this capacity what concerns would you have about the system proposed? What additional information would you require about the electronic voting system and what checks would you make before declaring the results of the vote?

[15]

(c) You are provided with suitable tools to create a 160-bit message digest, encryption using AES-128 and encryption and signatures using a 1024-bit RSA system. Explain how you make use of these tools in designing standard procedures to do the following:

(i) communicate confidential broadcast email securely to 100 recipients;

(ii) communicate financial transactions of 1000 bits in length which must not be altered in transit and which can be proved to have originated from a specific entity.

[6]

5. (a) What is meant by a public key infrastructure (PKI). Describe what options are available for implementing certificate hierarchies for a system designed to provide Secure Multipurpose Internet Mail Extensions (S/MIME)

[5]

(b) What is meant by a certificate revocation list (CRL) in a PKI? Explain why it is an essential feature of a PKI. Discuss how a CRL may be implemented securely.

[5]

(c) In the Kerberos system a ticket granting ticket is issued by the key distribution centre as a preliminary to the issue of a ticket which allows secure communication between two parties. What is the purpose of this preliminary stage? What keys are involved in this stage?

[5]

(d) Compare and contrast the PKIs that are used in Secure Sockets Layer (SSL) and Pretty Good Privacy (PGP).

[5]

(e) Explain how in Kerberos proxiable and forwardable ticket granting tickets may be used to sub-contract tasks securely in a network of computers.

[5]

6. (a) Figure 6.1 illustrates a system known as Lamport's Hash which can be used to provide secure access through a simple password and hash function. Explain how Lamport's Hash provides access and how it is secure against an interception type of attack and against an attack on the server database. Explain what is meant by a "small n attack" and what measures could be put in place to give protection against such an attack.

[7]

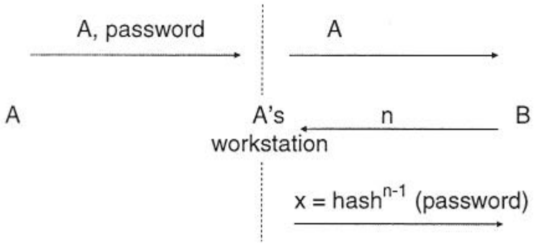


Figure 6.1 Lamport's Hash

(b) In the context of a system which relies on passwords, explain what is meant by a dictionary attack.

Passwords chosen by a community of users have on average an information content of 2 bits per character and are 6 characters long. Determine the size of a suitable dictionary which could be used to guess passwords used in the system.

[5]

(c) Explain what is meant by "perfect forward secrecy" and describe a simple system which exhibits this feature.

[4]

(d) Explain what is meant by a "denial of service" attack and describe ways in which protection can be provided against such an attack.

[4]

(e) Describe briefly a system which uses biometric information to authenticate people. What practical considerations have prevented the system you have described from achieving widespread use?

[5]

Network Security E4.44 | ISE 4.45 | S021
06 Answers

1(a) From Fig 1.1.

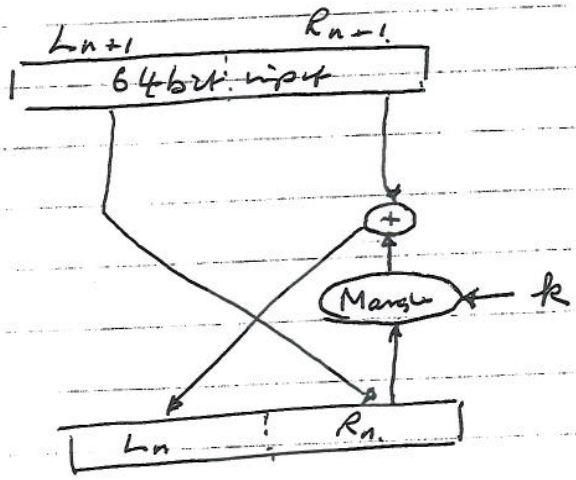
$$L_{n+1} = R_n \qquad (1)$$

$$R_{n+1} = L_n \oplus M_k(R_n). \qquad (2).$$

(1) is simply reversed for decryption whilst

$$L_n = R_{n+1} \oplus M_k(R_n) \qquad (3)$$

This gives the following diagram for decryption.



1(b) A weak key is one which is transformed into identical per-round keys. There are 4 weak keys:

28 zeroes : 28 ones
28 zeroes : 28 zeroes.
28 ones : 28 zeroes
28 ones : 28 ones.

Decryption is achieved ~~by~~ in DES by running through the same round structure with the keys in reverse. Since all per round keys are the same a weak key must be its own inverse.

1(c) ~~(i)~~ The number of keys involved in an exhaustive key search in the 4 methods is as follows

(i) DES	2^{56}
(ii) 3DES	2^{56}
(iii). IDEA	2^{56}
(iv). AES	2^{56}.

Therefore the relative strengths of the systems are ~~in the following~~ as follows

(i) DES C_D (ii) 3DES $3C_D$ (iii) IDEA C_I

(iv) AES C_A.

1(d). If the inverse of x^3+1 is $x^6+x^3+x^2+x+1$

then

$$(x^3+1)\times(x^6+x^3+x^2+x+1) = 1 \mod x^8+x^4+x^3+1$$

$$= x^9+x^6+x^5+x^4+x^3+x^6+x^3+x^2+x+1$$

$$= x^9+x^5+x^4+x^2+x+1$$

and taking this polynomial mod m(x)

$$\begin{array}{r} x \\ x^8+x^4+x^3+x+1\,\big)\,\overline{x^9+x^5+x^4+x^2+x+1} \\ \underline{x^9+x^5+x^4+x^2+x} \\ 1 \end{array}$$

Remainder $= 1$

$\therefore\ x^9+x^5+x^4+x^2+x+1 = 1 \mod x^8+x^4+x^3+1$

Second operation

$$(x^6 + x^3 + x^2 + x + 1)(x^4 + x^3 + x^2 + x + 1)$$

$$\begin{array}{l}
= \quad x^{10} + x^9 + x^8 + x^7 + x^6 \\
\quad\;\; x^7 + x^6 + x^5 + x^4 + x^3 \\
\quad\;\; x^6 + x^5 + x^4 + x^3 + x^2 \\
\quad\;\; x^5 + x^4 + x^3 + x^2 + x \\
\quad\;\; x^4 + x^3 + x^2 + x + 1.
\end{array}$$

$$= x^{10} + x^9 + x^8 + x^6 + x^5 + x^2 + 1$$

and dividing by $x^8 + 1$

$$\begin{array}{r r}
 & x^2 + x + 1 \\ \cline{2-2}
x^8 + 1 \,\big) & x^{10} + x^9 + x^8 + x^6 + x^5 + x^2 + 1, \\
 & x^{10} \qquad\qquad\qquad\qquad\quad + x^2 \\ \cline{2-2}
 & x^9 + x^8 + x^6 + x^5 + 1 \\
 & x^9 \qquad\qquad\qquad\quad + x \\ \cline{2-2}
 & x^8 + x^6 + x^5 + x + 1 \\
 & x^8 \qquad\qquad\qquad + 1 \\ \cline{2-2}
 & x^6 + x^5 + x.
\end{array}$$

Result of second operation is $x^6 + x^5 + x$.

2 (a).

Length of key is determined by the security strength required and the computing power available. That is it is a compromise between security strength and cost.

The maximum length of message block equals the key length

If the key length is 512 bits this will be the length of the cyphertext.

(b). ~~Any digital signature~~

If the message to be encrypted is of a standard type (eg one of n standard messages) it would be possible to guess the message encrypt it and (public keys are known to all) and compare with the cyphertext.

(c).

The public keys are T_A, T_B; g and p

The private keys are S_A and S_B

The public keys g and p are generally known in advance of the key exchange. The public keys T_A and T_B are calculated from the secret keys and are exchanged publicly. The secret keys S_A & S_B are not disclosed. As the system allows some keys to be made public whilst others are kept secret it may be categorised as a public key system.

An attacker sees T_A and T_B and would already know g and p. However in order to find S_A and S_B from T_A and T_B he would need to solve a discrete log problem which is computationally infeasible.

In a bucket brigade attack an interceptor C creates a false T_B for A and a false T_A for B. In this way he can set up secure communications with A and B who will believe incorrectly that they are talking to each other

$$\begin{tikzcd}
A \arrow[r, shift left, "T_A = g^{S_A} \bmod p"] & C \arrow[l, shift left, "T_B' = g^{S_{c1}} \bmod p"] \arrow[r, shift left, "T_A' = g^{S_{c2}} \bmod p"] & B \arrow[l, shift left, "T_B = g^{S_B} \bmod p"]
\end{tikzcd}$$

$$K_1 = g^{S_A} g^{S_{c1}} \qquad k_2 = g^{S_B S_{c2}}$$

To protect against a bucket brigade attack A and B should sign their messages thus authenticating themselves or alternatively encrypt their communications with the other's public key.

(d).
$$X = S_m^{-1}(d_m + S\,T_m) \bmod q$$

$$\therefore S_m X = (d_m + S\,T_m) \bmod q$$

$$S = (S_m X - d_m)T_m^{-1} \bmod q.$$

If we have two signatures X_{m_1} and X_{m_2} which use the same per message secret S_m (and therefore the same $T_m = (g^{S_m} \bmod p) \bmod q$ then we may form the equality

$$X_{m_2} - X_{m_1} = S_m^{-1}(d_{m_2} - d_{m_1}) \bmod q$$

$$\text{or } S_m = (X_{m_2} - X_{m_1})^{-1}(d_{m_2} - d_{m_1}) \bmod q$$

Since we can calculate Sm we may calculate the long term secret S as shown above.

3(a).

'Endpoint Identifier Hiding' prevents an observer of a communication from ascertaining the identities of the parties involved. In Phase 1 IKE crypto negotiation and a Diffie Hellman key exchange takes place anonymously and disclosure of identities takes place under the security of a Diffie Hellman session key and a long term key.

In Phase 1 IKE proof of identity (the last two lines of the protocol) comprises a hash of the following: long term key, Diffie Hellm values, once only nonces and crypto choices.

(b) ESP is a protocol of IPSec which allows for encryption of the message data and authentication of the message data. AH allows only authentication of the data. A possible advantage over an authentication only system is that level 4 information is guaranteed to be available to routers and other network devices which use level 4 information for QOS.

In tunnel mode an entire IP packet is treated as data for a new packet which has its own address and control information in addition to IP Sec security.

Tunnel mode is useful to secure a particular route through a network as, for example, may be required between two firewalls.

(c)

(i) The firewall should be set up as a packet filter and should examine all source addresses from outside the LAN and all destination addresses from inside the LAN. Any packets containing the offending address would be dropped.

(ii) The firewall should examine the level 4 port information for all incoming packets and block all sessions indicating that TELNET protocol is being used.

(iii) The first TCP packet initialising a session would not have the Ack bit set. All such incoming packets should be barred.

(d) HTTP Digest Authentication uses a hash function ~~not~~ of amongst others the user's name and password, a once only number and the URL. This is simple and cheap to produce. By contrast SSL uses a full public key system requiring certificates and trust anchors.

HTTP provides protection from a replay attack by the use of once only numbers which are incremented at each transaction.

Protection against database disclosure is arranged by storing a hash of the password and name.

~~9~~ 8

4 (a) If the number of people in a room exceeds 23 there is a very good chance that two of them will have the same birthday. In the context of message digests the probability that two messages have the same N-bit message digest is $1/2^{N/2}$. A safe length for a message digest would be in excess of 128 bits. In this case the probability that any two messages have the same digest is 2^{-64}

4(b).

The main problem with the proposed system is that the IDs would be available to someone intent on manipulating the vote and the passwords may be calculated from the ID. This could enable false votes to be recorded and, depending upon what checks are made, could prevent legitimate shareholders from voting. If the system does not give any feedback to the voter that the vote has been accepted or rejected the voter would not know if he had been disenfranchised by a fraudster. Addit the votes could be manipulated by the company.

Therefore the main concern are

- shareholders may be impersonated
- multiple votes may be recorded for the same shareholder account
- A shareholder's voting rights ~~can~~ might be stolen without his knowledge
- the company or its employees might attemp. ~~Further information~~ to falsify the returns.

Questions that should be asked include the following.

— why were passwords not chosen randomly?

— who manages the system used for electronic voting?

— Are checks made to ensure that a shareholder registers only one vote?

— If checks are made ~~is the~~ does the system inform the shareholder that his vote has been rejected?

Before declaring the result it would be prudent to visit the location which houses the computer system and to interview the staff who manage it. It would be prudent to insist on examining a record of all votes cast against shareholder number and to compare with the official number for votes cast.

4(c)

(i) ~~For~~ Make a message digest of the message and sign this with the RSA system using the private key. Encrypt the ~~message digest with and message~~ message with its signature using AES-128 with a randomly chosen key. Send the random key encrypted under the RSA public key of each individual recipient.

(ii). Sign the transactions directly with the RSA private key.

5 (a). A PKI is a system for ensuring that public keys can be trusted. It comprises public key certificates, a mean for issuing certificates a means of revoking certificates and a method for qualifying trust in a certificate.

The options for certificate hierarchies are as follows: public certifiers, organisational certifiers or any informal system of certification authorities. Public certifiers are companies whose business is issuing certificates. An organisational certifier would be a company division or authority that employs the owners of public keys. An informal system would resemble that used in PGP.

5 (b). A certificate revocation list provides informt on all certificates whose validity has been revoked. The options are :-

— Delta CRLs in which only those certificates revoked since the last list would be included

— On-line schemes from which information on any revoked certificate can be obtained

— Publication of a full 'bad list' of revoked certificates.

5 (c) The purpose of the first stage is to authenticate the user and to supply a session key for next stage. It serves to keep the KDC stateless as the TGT contains all the informt the KDC will need for the second stage. Infom returned by the KDC is encrypted under t user's master key and contains the session +

for the next stage are the TGT which itself contains the session key and is encrypted under the KDC master key. In summary the keys used are users master key an the KDC's master key

d). SSL uses a PKI based on the oligarchy model whilst PGP's PKI is based on the anarchy model. In the oligarchy model the user has a number of trust anchors and will accept a certificate issued by any trust anchor. The security strength of the system is defined by the quality of the trust anchors and can be controlled. By contrast PGP allows certificates from any source and the user must make his own judgement. Such judgement may be based on very little information.

e) A forwardable TGT is one that may be exchanged for a TGT with a different network address. Tickets to allow secure access to a remote resource can then be granted.

A proxiable TGT is one which can be used to go request tickets for use ~~with~~ from a different network address. This allows the a sub-contractor to use TGTs requested by another to gain tickets to allow secure access from his own address.

~~B~~ 12

6.

6(a) Lamports Hash works in the follows wa

A requests communication with a serve which returns a number n. A creates a numbe formed by hashing his password n-1 times. On receipt of this the server hashes it one more time and compares the result to hash^n (password) which he has kept in ~~store~~ database. If it matches then access is granted and the server database replies n with n-1 and hash^n(passw) with hash^{n-1}(password)

~~The~~ An observer seeing hash^{n-1}(password) cannot ~~create~~ calculate the password. ~~I~~ An attack on the database reveals only hash^n(password) from which the password cannot be obtained.

In a small n attack an attacker impersonates the server and gives the user a small n from which he ~~o~~ receives hash^{n-k}(password) in return. He can now form hash^n(password) for a large value of n.

To protect against this type of attack the user should keep a record of values of n used.

(b) A dictionary attack is an exhaustive he search for passwords. ~~If~~ Any information on how passwords are chosen reduces the size of the dictionary.

Information in the passwd is 12 bits. The size of the dictionary should therefore be of the order of 4096 $(= 2^{12})$

6(c) Perfect forward secrecy is the property ~~in~~ ~~which~~ which prevents the record of a secure communication being decoded after a machine's database has been compromised. A simple way of providing perfect forward secrecy is to use randomly chosen session keys ~~which should be destroy~~ (e.g. from a Diffie Hellman key exchange) which should be destroyed after the session.

(d) A denial of service attack is one in which server congestion is created artificially by bogus requests from (usually) false IP addresses. Denial of Service attacks are difficult to prevent but some protection may be offered by bringing in a second stage to the initial service request. The second stage involves a reply to the originating address requesting the completion of a task which is difficult to complete but easy to check (e.g finding a message for a message digest).

(e). Any system such as iris scanners, voiceprints or signatures will be acceptable. A discussion of the practicalities should include reference to false acceptance / false rejection ratios.