

Question Paper

Cryptography and Computer Security (MB361IT) : April 2008

Section A : Basic Concepts (30 Marks)

- This section consists of questions with serial number 1 - 30.
- Answer all questions.
- Each question carries one mark.
- Maximum time for answering Section A is 30 Minutes.

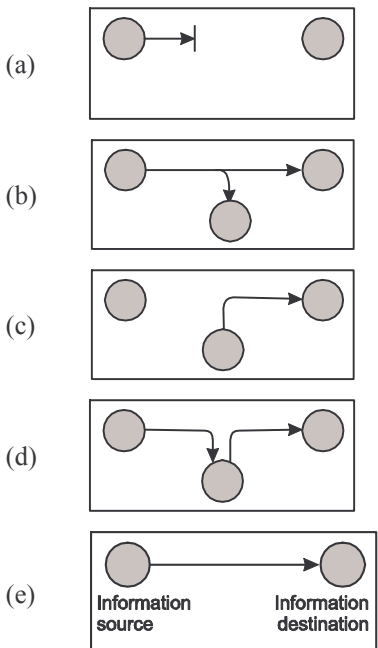
1. Which of the following aspects of information security is designed to detect, prevent or recover from a security attack? [<Answer>](#)

- (a) Security mechanism
- (b) Security attack
- (c) Security service
- (d) Security recovery
- (e) Security identification.

2. In which of the following security threats, an authorized party gains access to an asset? [<Answer>](#)

- (a) Interruption
- (b) Interception
- (c) Concurrence
- (d) Modification
- (e) Fabrication.

3. Which of the following figures of security threat represents modification? [<Answer>](#)



4. Which of the following is **not** an active attack? [<Answer>](#)

- (a) Masquerade
- (b) Replay
- (c) Traffic analysis
- (d) Denial of service
- (e) Modification of messages.

5. Which of the following is responsible for technical management of Internet Engineering Task Force activities and the Internet Standards Process? [<Answer>](#)

- (a) Internet Architecture Board

- (b) Internet Engineering Board
- (c) Internet Engineering Steering Group
- (d) Internet Architecture Task Force
- (e) Internet Architecture Steering Group.

6. A hash function (H) that satisfies the following six properties is referred to as

[<Answer>](#)

- i. H can be applied to a block of data of any size.
- ii. H produces a fixed-length output.
- iii. $H(x)$ is relatively easy to compute for any given x , making both hardware and software implementations practical.
- iv. For any given code h , it is computationally infeasible to find x such that $H(x)=h$.
- v. For any given block x , it is computationally infeasible to find $y \neq x$ with $H(y)=H(x)$.
- vi. It is computationally infeasible to find any pair (x, y) such that $H(x)=H(y)$.

- (a) Strong hash function
- (b) Weak hash function
- (c) Virtual hash function
- (d) Dependent hash function
- (e) Independent hash function.

7. In Pretty Good Privacy (PGP) which of the following indicates compression?

[<Answer>](#)

- (a) C
- (b) C^{-1}
- (c) Z
- (d) Z^{-1}
- (e) D .

8. In MD5 algorithm, the input is processed in

[<Answer>](#)

- (a) 32 bit blocks
- (b) 64 bit blocks
- (c) 128 bit blocks
- (d) 256 bit blocks
- (e) 512 bit blocks.

9. IPv6 Header has a fixed length of 40 octets and it contains 8 fields. The Flow Label field consists of

[<Answer>](#)

- (a) 4 bits
- (b) 8 bits
- (c) 16 bits
- (d) 20 bits
- (e) 128 bits.

10. In RSA Public-Key Encryption, if we select two prime numbers p and q as 3 and 5, then find the value of n .

[<Answer>](#)

- (a) 8
- (b) 2
- (c) 15
- (d) 125
- (e) 243.

11. In RSA Public-Key Encryption, if we select two prime numbers p and q as 5 and 7, then find the value of $\phi(n)$.

[<Answer>](#)

- (a) 12
- (b) 2
- (c) 35
- (d) 24
- (e) 32.

12. In which of the following phases the virus performs the function, which may be harmless such as a message on the screen or harmful such as destructive of programs and data files?

[<Answer>](#)

- (a) Dormant phase
- (b) Propagation phase
- (c) Triggering phase
- (d) Execution phase

- (d) Execution phase
- (e) Active phase.

13. Which of the following is/are **not** the fields of IPv4 Header?

[<Answer>](#)

- I. Version.
- II. Padding.
- III. Time to Live.
- IV. Hop Limit.
- V. Flags.

- (a) Only (I) above.
- (b) Only (III) above
- (c) Only (IV) above
- (d) Both (I) and (II) above
- (e) Both (III) and (V) above.

14. Which of the following Kerberos version5 flags tells Ticket-Granting-Server (TGS) that a new service-granting ticket with a different network address may be issued based on the presented ticket?

[<Answer>](#)

- (a) INVALID
- (b) PROXIABLE
- (c) PRE-AUTHENT
- (d) HW-AUTHENT
- (e) POSTDATED.

15. Content-Transfer-Encoding field can actually take on six values. Which of the following value encodes data by mapping 6-bit blocks of input to 8-bit blocks of output, all of which are printable ASCII characters?

[<Answer>](#)

- (a) 7 bit
- (b) 8 bit
- (c) binary
- (d) base64
- (e) x-token.

16. Which of the following IPSec document describes the specification of key management capabilities?

[<Answer>](#)

- (a) RFC 2401
- (b) RFC 2402
- (c) RFC 2104
- (d) RFC 2406
- (e) RFC 2408.

17. In IPSec Encapsulating Security Payload (ESP) format, Sequence number field consists of

[<Answer>](#)

- (a) 8 bits
- (b) 32 bits
- (c) 64 bits
- (d) 128 bits
- (e) 256 bits.

18. The default automated key management protocol for IPSec is referred to as Internet Security Association and Key Management Protocol (ISAKMP). In ISAKMP header format, what is the size of Message ID field?

[<Answer>](#)

- (a) 8 bits
- (b) 32 bits
- (c) 64 bits
- (d) 128 bits
- (e) 256 bits.

19. The default automated key management protocol for IPSec is referred to as Internet Security Association and Key Management Protocol (ISAKMP). Which of the following ISAKMP Payload types indicate a Security Association (SA) that is no longer valid?

[<Answer>](#)

- (a) Proposal
- (b) Transform
- (c) Notification
- (d) Delete
- (e) Nonce.

20. What is the key size in the conventional encryption algorithm IDEA?

[<Answer>](#)

- (a) 42 bits
- (b) 56 bits
- (c) 112 bits
- (d) 128 bits
- (e) 168 bits.

21. What is the maximum message size in MD5 algorithm?

[<Answer>](#)

- (a) ∞
- (b) $2^{64} - 1$ bits
- (c) $2^{32} + 1$ bits
- (d) $2^{64} + 1$ bits
- (e) $2^{32} - 1$ bits.

22. PGP provides various functions. Which of the following algorithms is used for the function “E-mail compatibility” in PGP?

[<Answer>](#)

- (a) DSS
- (b) CAST
- (c) Radix-64 conversion
- (d) ZIP
- (e) SHA.

23. Which type of virus attaches itself to executable files and replicates when the infected program is executed, by finding other executable files to infect?

[<Answer>](#)

- (a) Parasitic virus
- (b) Memory-resident virus
- (c) Polymorphic virus
- (d) Stealth virus
- (e) Boot sector virus.

24. Which generation scanner uses heuristic rules to search for probable virus infection?

[<Answer>](#)

- (a) First generation
- (b) Second generation
- (c) Third generation
- (d) Fourth generation
- (e) Fifth generation.

25. Which of the following type of firewall is also called proxy server?

[<Answer>](#)

- (a) Packet filtering router
- (b) Direction-level gateway
- (c) Application-level gateway
- (d) Service filtering router
- (e) Circuit-level gateway.

26. Blowfish Conventional encryption algorithm was developed by

[<Answer>](#)

- (a) Carlisle Adams
- (b) Xuejia Lai
- (c) Tauchman
- (d) Bruce Schneier
- (e) Ron Rivest.

27. Which of the following MIME header field indicate the type of transformation that has been used to represent the body of the message in a way that it is acceptable for mail transport?

[<Answer>](#)

- (a) MIME-Version
- (b) Content-Type
- (c) Content-Transfer-Encoding
- (d) Content-ID
- (e) Content-Description.

[<Answer>](#)

28. Conventional encryption also referred to as

- I. Symmetric encryption.
 - II. Secret key encryption.
 - III. Single-key encryption.
 - IV. Asymmetric encryption.
- (a) Only (I) above
 - (b) Only (II) above
 - (c) Both (II) and (IV) above
 - (d) (I), (II) and (III) above
 - (e) (II), (III) and (IV) above.

[<Answer>](#)

29. Which of the following function is used to calculate the message authentication code MAC_M , if A has a message to send to B and K_{AB} is the common secret key?

- (a) $F(K_{AB}, M)$
- (b) $F(K_{AB}, M_{AB})$
- (c) $F(M_A, M_B)$
- (d) $F(K_{AB} \times M_{AB})$
- (e) $F(K_{AB} / M_{AB})$.

[<Answer>](#)

30. In RIPEMD-160 message-digest algorithm the input is processed in

- (a) 4 bit blocks
- (b) 128 bit blocks
- (c) 160 bit blocks
- (d) 512 bit blocks
- (e) 2^{64} bit blocks.

END OF SECTION A

Section B : Caselets (50 Marks)

- This section consists of questions with serial number 1 – 5.
- Answer all questions.
- Marks are indicated against each question.
- Detailed explanations should form part of your answer.
- Do not spend more than 110 - 120 minutes on Section B.

Caselet 1

Read the caselet carefully and answer the following questions:

1. What are the security services that Alpa Solutions might have provided to the client? Explain. [<Answer>](#)
(8 marks)
2. In the caselet, Alpa Solutions has chosen TDEA for protecting sensitive data over network. Explain why Alpa Solutions has chosen TDEA. [<Answer>](#)
(10 marks)
3. In the caselet it is given that “Client is a US-based maker of networking equipment, and offers products and solutions in the areas of voice and IP Communications and Wireless”. If you are the security manager at Alpa Solutions, how will you provide security in wireless networks? [<Answer>](#)
(12 marks)

The client is a US-based maker of networking equipment and offers products and solutions in the areas of broadband, content networking, DSL, optical networking, voice and IP Communications and Wireless. The company also has a range of security products and services to safeguard systems from unauthorized usage. It

engaged Alpa Solutions to create a robust security platform that would support its range of security products.

The Alpa Solutions addressed speed (through a software compression algorithm), security and ensured that the hardware seamlessly interfaced with protocols such as TCP/IP, VPN/Security and ISAKMP. Security was guaranteed by utilizing security algorithms such as the MD5 algorithm, DES (Data Encryption Standard), TDEA and by carefully blending cryptography technologies. Alpa has considered TDEA for protecting sensitive data over network. Security services taken by the Alpa Solutions enhances the security of data processing systems and the information of an organization. The services are intended to counter security attacks and they make use of one/more security mechanisms to provide the service.

Alpa Solutions delivered several benefits:

- Costs were reduced, while quality was enhanced.
- In addition to security, speed is critical for QoS (Quality of Service) applications like RTP (Real-Time Transport Protocol), which are used for real-time video and audio over the Internet. Alpa Solutions code ensured that RTP applications were not hampered, and this boosted both speed and safety for the client's customers.

Usage of an innovative cache for the security association database on the crypto accelerator further improved speed and ensured that the overall throughput was much greater than that provided by the client's competitors.

**END OF
CASELET 1**

Caselet 2

Read the caselet carefully and answer the following questions:

4. The introduction of Secure Socket Layer (SSL) technology brings secure, dependable remote access that is less expensive than IPSec or Leased Line VPNs. Explain the important concepts of SSL and their parameters. (12 marks) [<Answer>](#)
5. Explain about the remote access product provided by TEXAS Systems. Did the product satisfy Ceer consulting firm? (8 marks) [<Answer>](#)

Ceer Consulting is a strategy and technology consulting firm that offers services in business performance improvement. Ceer's clients include Fortune 1000 and mid-market companies in Pharmaceuticals and Healthcare, Media and Entertainment, Financial Services, Retail and Consumer Goods, Hi-Tech and Commercial Products & Services. Ceer helps clients build effective business solutions that drive business performance and cultivate long-term relationships with valuable customers.

The demand for remote access to corporate e-mail and other internal applications has grown exponentially in the last decade. Ceer Consulting works at the national level and oftentimes away from its corporate offices in Chicago, Boston, Indianapolis, New York and Dallas. With over 160 consultants in the field, e-mail access is a key requirement for the company. Ceer's Director of Network Services, Mr.Beth, was looking for a solution that would allow employees to securely send and receive e-mail directly from their laptops while working at varied locations, including client offices, hotel rooms, Internet cafes and other hotspots.

Ceer Consulting's original Virtual Private Network (VPN) provided unstable and unsecured access to corporate e-mail. Consultants in the field were often unable to connect to the VPN, distracting them from their clients' needs as they would try to communicate with their home office. Ceer needed a secure, reliable VPN that provided access to e-mail from anywhere on the Internet, and at a cost that was affordable. The introduction of Secure Socket Layer (SSL) technology brings secure, dependable remote access that is less expensive than IPSec or Leased Line VPNs. However, the average cost of an SSL VPN still ranges from \$20,000 - \$40,000 to implement. Despite the increasing number of SSL VPN vendors in the market, most solutions are out of reach for Small and Medium-sized Businesses (SMBs).

TEXAS SureWare B-Gate AG-600 offered Ceer Consulting security, reliability and

affordability – all key elements for communicating with consultants in the field. SureWare B-Gate provides simple administration, a user-based installation and accessibility to corporate resources from anywhere at anytime. Beth first looked at SureWare B-Gate because TEXAS Systems' SSL accelerator cards (SureWare Runner) are well respected in the marketplace. "It made sense to me to purchase an SSL VPN from a company that knows high-performance SSL. TEXAS Systems is a company that has an excellent reputation in the SSL market, so it seemed a natural choice to look at their SSL VPN product."

Ceer Consulting chose TEXAS Systems' SureWare B-Gate as a reliable, secure remote access solution that saved the company money in acquisition and maintenance costs, was easy to install and provided functionality that increased company productivity and decreased resource demands. Here's how they did it. SureWare B-Gate's SSL VPN appliance gives a higher return on investment than a traditional remote access system because its acquisition cost is significantly lower than an equivalent IPSec system and its maintenance costs are minimal. Users are added at no additional cost.

In addition to SureWare B-Gate's reliability and affordability, the virtual network offers flexibility in its services and accessibility to the corporate network. As Ceer Consulting continues to grow, it can expand its use of SureWare B-Gate to include more than e-mail access. Employees can also access applications including Lotus Notes, Microsoft Word, Microsoft Excel and legacy applications.

SureWare B-Gate is aimed at small and mid-sized businesses that have minimal IT staff, but so easy deployment is the key. According to Beth, Ceer Consulting's SureWare B-Gate was installed, configured and providing access to remote workers all within two hours. Since its installation, SureWare B-Gate has effectively and reliably handled all e-mail requirements for its remote staff.

"The new SSL VPN is excellent and the client install was easy. In the past I was sometimes unable to connect using our previous VPN, but so far this new SSL VPN solution has always worked. Being able to connect regularly while on the road allows us to focus on the work at hand and not on where we can find a place to 'phone home'," said John, Senior Vice President of the Enabling Technology Group at Ceer Consulting.

"The B-Gate option was the best way to create an SSL connection from a client anywhere on the Internet back to our exchange server, a connection that is secure and can go anywhere. We haven't had any problems getting remote access up and running on any laptops. Not one failure. No one from anywhere on the planet has told us that their B-Gate connection doesn't work," said Beth. The TEXAS SureWare B-Gate solution has increased company productivity and reduced the demand for network storage because it allows the full use of the Outlook client. Now Ceer's consultants can download their e-mail and take it with them, and view e-mail at their client sites - functionality that Ceer's in-the-field staff did not have before. "We could have paid a lot of money to solve our e-mail problem. But implementing B-Gate was a brilliant solution. We found a very solid product with good functionality for a price we could afford," said Beth.

**END OF
CASELET 2**

END OF SECTION B

Section C : Applied Theory (20 Marks)

- This section consists of questions with serial number 6 - 7.
- Answer all questions.
- Marks are indicated against each question.
- Do not spend more than 25 - 30 minutes on Section C.

6. Pretty Good Privacy (PGP) provides confidentiality and authentication service that can be used for electronic mail and file storage applications. Discuss the various services provided by PGP. [<Answer>](#) (10 marks)

7. Write short notes on: [<Answer>](#)
- Trap doors.
 - Logic Bomb.
 - Trojan Horses.
 - Viruses.
 - Worms.
- (10 marks)

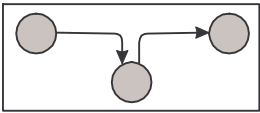
END OF SECTION C

END OF QUESTION PAPER

Suggested Answers

Cryptography and Computer Security (MB361IT) : April 2008

Section A : Basic Concepts

- | Answer | Reason |
|--------|--|
| 1. A | Security mechanism: A mechanism that is designed to detect, prevent or recover from a security attack. < TOP > |
| 2. B | Interception: An authorized party gains access to an asset. This is an attack on confidentiality. < TOP > |
| 3. D | <div style="display: flex; align-items: center;">  represents modification. </div> < TOP > |
| 4. C | Traffic analysis is not an active attack. It is a passive attack. < TOP > |
| 5. C | Internet Engineering Steering Group is responsible for technical management of Internet Engineering Task Force activities and the Internet standards process. < TOP > |
| 6. A | Strong hash function satisfies all the following properties. < TOP > <ol style="list-style-type: none"> H can be applied to a block of data of any size. H produces a fixed-length output. $H(x)$ is relatively easy to compute for any given x, making both hardware and software implementations practical. For any given code h, it is computationally infeasible to find x such that $H(x)=h$. For any given block x, it is computationally infeasible to find $y \neq x$ with $H(y)=H(x)$. It is computationally infeasible to find any pair (x,y) such that $H(x)=H(y)$. |
| 7. C | In PGP compression is represented by Z . < TOP > |
| 8. E | In MD5 algorithm, the input is processed in 512 bit blocks. < TOP > |
| 9. D | The Flow Label field consists of 20 bits. < TOP > |
| 10. C | Given $P = 3, q = 5, n = pq$
$= (3)(5) = 15$. < TOP > |
| 11. D | Given $P = 5, q = 7$,
$\phi(n) = (p-1)(q-1)$ (Euler's function)
$= (5-1)(7-1)$ < TOP > |

$$= (4)(6) = 24.$$

12. D In Execution phase the virus performs the function, which may be harmless such as a message on the screen or harmful such as destructive of programs and data files. [< TOP >](#)
13. C Hop Limit is not the field in IPv4 Header. It is the field in IPv6 header. [< TOP >](#)
14. B PROXIABLE flag tells Ticket-Granting-Server that a new ticket with a different network addresses may be issued based on the presented ticket. [< TOP >](#)
15. D base64: encodes data by mapping 6-bit blocks of input to 8-bit blocks of output, all of which are printable ASCII characters. [< TOP >](#)
16. E RFC 2408 describes the specification of key management capabilities. [< TOP >](#)
17. B In IPSec Encapsulating Security Payload (ESP) format, Sequence number consists of 32 bits. [< TOP >](#)
18. B In ISAKMP header format, the size of Message ID field is 32 bits. [< TOP >](#)
19. D Proposal Payload type indicates protocol for Security Association (SA) for which services and mechanisms are being negotiated.
Delete Payload type indicates a Security Association (SA) that is no longer valid.
Transform Payload type indicates transform and related SA attributes.
Notification Payload type used to transmit notification data, such as an error condition.
Nonce Payload type contains a nonce. [< TOP >](#)
20. D Key size in the conventional encryption algorithm IDEA is 128 bits. [< TOP >](#)
21. A Maximum message size in MD5 algorithm is ∞ . [< TOP >](#)
22. C The function of Radix-64 conversion is E-mail compatibility. [< TOP >](#)
23. A Parasitic virus attaches itself to executable files and replicates, when the infected program is executed, by finding other executable files to infect. [< TOP >](#)
24. B Second generation scanner uses heuristic rules to search for probable virus infection. [< TOP >](#)
25. C Application-level gateway also called proxy server. [< TOP >](#)
26. D Blowfish Conventional encryption algorithm was developed by Bruce Schneier. [< TOP >](#)
27. C Content-Transfer-Encoding indicates the type of transformation that has been used to represent the body of the message in a way that is acceptable for mail transport. [< TOP >](#)
28. D Conventional encryption also referred to as symmetric encryption, secret key encryption, single-key encryption. [< TOP >](#)
29. A If A has a message M to send to B, if K_{AB} is the common secret key, then the function of message authentication code is calculated as $F(K_{AB}, M)$. [< TOP >](#)
30. D In RIPEMD-160 message digest algorithm, the input is processed in 512 bit blocks. [< TOP >](#)

Section B : Caselets

1. The security services that Alpa solutions might have provided to the client are:

[< TOP >](#)

- Confidentiality
- Authentication
- Integrity
- Nonrepudiation
- Access control
- Availability

Confidentiality

Confidentiality is the protection of transmitted data from passive attacks. With respect to the release of message contents, several levels of protection can be identified. The broadest service protects all user data transmitted between two users over a period of time. For example, if a virtual circuit is set up between two systems, this broad protection would prevent the release of any user data transmitted over the virtual circuit. Narrower forms of this service can also be defined, including the protection of a single message or even specific fields within a message. These refinements are less useful than the broad approach and may even be more complex and expensive to implement.

Authentication

The authentication service is concerned with assuring that a communication is authentic. In the case of a single message, such as a warning or alarm signal, the function of the authentication service is to assure the recipient that the message is from the source that it claims to be from. In the case of an ongoing interaction, such as the connection of a terminal to a host, two aspects are involved. First, at the time of connection initiation, the service assures that the two entities are authentic (that is, that each is the entity that it claims to be). Second, the service must assure that the connection is not interfered with in such a way that a third party can masquerade as one of the two legitimate parties for the purposes of unauthorized transmission or reception.

Integrity

As with confidentiality, integrity can apply to a stream of messages, a single message, or selected fields within a message. Again, the most useful and straightforward approach is total stream protection.

A connection-oriented integrity service, one that deals with a stream of messages, assures that messages are received as sent, with no duplication, insertion, modification, reordering, or replays. The destruction of data is also covered under this service. Thus, the connection oriented integrity service addresses both message stream modification and denial of service. On the other hand, a connectionless integrity service, one that deals with individual messages only without regard to any larger context, generally provides protection against message modification only.

We can make a distinction between the service with and without recovery. Because the integrity service relates to active attacks, we are concerned with detection rather than prevention. If a violation of integrity is detected, then the service may simply report this violation, and some other portion of software or human intervention is required to recover from the violation. Alternatively, there are mechanisms available to recover from the loss of integrity of data, as we will review subsequently. The incorporation of automated recovery mechanisms is, in general, the more attractive alternative.

Nonrepudiation

Nonrepudiation prevents either sender or receiver from denying a transmitted message. Thus, when a message is sent, the receiver can prove that the message was in fact sent by the alleged sender. Similarly, when a message is received, the sender can prove that the message was in fact received by the alleged receiver.

Access Control

In the context of network security, access control is the ability to limit and control the access to host systems and applications via communications links. To achieve this control, each entity trying to gain access must first be identified, or authenticated, so that access rights can be

tailored to the individual.

Availability

A variety of attacks can result in the loss of or reduction in availability. Some of these attacks are amenable to automated countermeasures, such as authentication and encryption, whereas others require some sort of physical action to prevent or recover from loss of availability of elements of a distributed system.

2. TDEA uses three keys and three executions of the DES algorithm. The function follows an encrypt-decrypt-encrypt (EDE) sequence (Figure):

[< TOP >](#)

$$C = E_{K_3} [D_{K_2} [E_{K_1} [P]]]$$

where

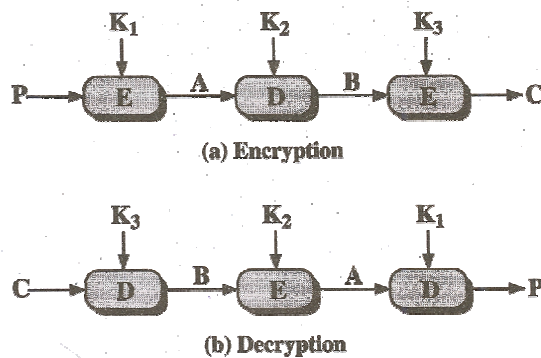
C = ciphertext

P = plaintext

EK[X] = encryption of X using key K DK[Y] = decryption of Y using key K

Decryption is simply the same operation with the keys reversed (Figure):

$$P = D_{K_1} [E_{K_2} [D_{K_3} [C]]]$$



There is no cryptographic significance to the use of decryption for the second stage of TDEA encryption. Its only advantage is that it allows users of IDEA to decrypt data encrypted by users of the older single DES:

$$C = E_{K_1} [D_{K_1} [E_{K_1} [P]]] = E_{K_1} [P]$$

With three distinct keys, IDEA has an effective key length of 168 bits. FIPS 46-3 also allows for the use of two keys, with $K_1 = K_3$; this provides for a key length of 112 bits. FIPS 46-3 includes the following guidelines for IDEA:

- IDEA is the FIPS approved conventional encryption algorithm of choice.
- The original DEA, which uses a single 56-bit key, is permitted under the standard for legacy systems only. New procurements should support IDEA.
- Government organizations with legacy DEA systems are encouraged to transition to IDEA.
- It is anticipated that IDEA and the advanced encryption standard (AES) will coexist as FIPS-approved algorithms, allowing for a gradual transition to AES.

It is easy to see that IDEA is a formidable algorithm. Because the underlying cryptographic algorithm is DEA, TDEA can claim the same resistance to cryptanalysis based on the algorithm as is claimed for DEA. Further, with a 168-bit key length, brute-force attacks are effectively impossible.

Advanced Encryption Standard

TDEA has two attractions, that might have impresses Alpha Solutions. First, with its 168-bit key length, it overcomes the vulnerability to brute-force attack of DEA. Second, the underlying encryption algorithm in IDEA is the same as in DEA. This algorithm has been subjected to more scrutiny than any other encryption algorithm over a longer period of time, and no effective cryptanalytic attack based on the algorithm rather than brute force has been found. Accordingly, there is a high level of confidence that TDEA is very resistant to cryptanalysis. In

the caselet security was the only consideration that is the reason Alpa Solutions has chosen TDEA.

3. If I am the security manager at Alpa Solutions, I will provide security in wireless networks by [< TOP >](#) using following steps.

Change the System ID: Devices come with a default system ID called the SSID (Service Set Identifier) or ESSID (Extended Service Set Identifier). It is easy for a hacker to find out what the default identifier is for each manufacturer of wireless equipment so I will change this to something else. Use something unique-not your name or something easily guessed.

Disable Identifier Broadcasting: Announcing that I have a wireless connection to the world is an invitation for hackers. I already know I have one so I don't need to broadcast it. I will check the hardware and figure out how to disable broadcasting.

Enable Encryption: WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected Access) encrypt your data so that only the intended recipient is supposed to be able to read it. WEP has many holes and is easily cracked. 128-bit keys impact performance slightly without a significant increase in security so 40-bit (or 64-bit on some equipment) encryption is just as well. As with all security measures there are ways around it, but by using encryption I will keep the casual hackers out of our systems. If possible, I will use WPA encryption (most older equipment can be upgraded to be WPA compatible). WPA fixes the security flaws in WEP but it is still subject to DOS (denial-of-service) attacks.

Restrict Unnecessary Traffic: Many wired and wireless routers have built-in firewalls. They are not the most technically advanced firewalls, but they help create one more line of defense. I will read the manual for my hardware and learn how to configure my router to only allow incoming or outgoing traffic that I have approved.

Change the Default Administrator Password: This is just good practice for ALL hardware and software. The default passwords are easily obtained and because so many people don't bother to take the simple step of changing them they are usually what hackers try first. Make sure that I change the default password on my wireless router / access point to something that is not easily guessed like my last name.

Patch and Protect Your PC's: As a last line of defense I will have personal firewall software such as Zone Alarm Pro and anti-virus software installed on my computer. As important as installing the anti-virus software, I will keep it up to date. New viruses are discovered daily and anti-virus software vendors generally release updates at least once a week. I will also keep up to date with patches for known security vulnerabilities.

4. The important concepts of Secure Socket Layer (SSL) and their parameters are: [< TOP >](#)

- **Connection:** A connection is a transport (in the OSI layering model definition) that provides a suitable type of service. For SSL, such connections are peer-to-peer relationships. The connections are transient. Every connection is associated with one session.
- **Session:** An SSL session is an association between a client and a server. Sessions are created by the Handshake Protocol. Sessions define a set of cryptographic security parameters, which can be shared among multiple connections. Sessions are used to avoid the expensive negotiation of new security parameters for each connection.

A session state is defined by the following parameters

- **Session identifier:** An arbitrary byte sequence chosen by the server to identify an active or resumable session state.
- **Peer certificate:** An X509.v3 certificate of the peer. This element of the state may be null.
- **Compression method:** The algorithm used to compress data prior to encryption.
- **Cipher spec:** Specifies the bulk data encryption algorithm (such as null, DES, etc) and a hash algorithm (such as MD5 or SHA-1) used for MAC calculation. It also defines cryptographic attributes such as the hash size.
- **Master secret:** 48-byte secret shared between the client and server.
- **Is resumable:** A flag-indicating whether the session can be used to initiate new connections.

A connection state is defined by the following parameters.

- **Server and client random:** Byte sequences that are chosen by the server and client for each connection.
 - **Server write MAC secret:** The secret key used in MAC operations on data sent by the server.
 - **Client write MAC secret:** The secret key used in MAC operations on data sent by the client.
 - **Server write key:** The conventional encryption for data encrypted by the server and decrypted by the client.
 - **Client write key:** The conventional encryption key for data encrypted by the client and decrypted by the server.
 - **Initialization vectors:** When a block cipher in CBC mode is used, an initialization vector (IV) is maintained for each key. This field is first initialized by the SSL Handshake Protocol. Thereafter the final cipher text block from each record is preserved for use as the IV with the following record.
 - **Sequence numbers:** Each party maintains separate sequence numbers for transmitted and received messages for each connection. When a party sends or receives a change cipher spec message, the appropriate sequence number is set to zero.
5. TEXAS SureWare B-Gate AG-600 offered Ceer Consulting security, reliability and affordability - all key elements for communicating with consultants in the field. SureWare B-Gate provides simple administration, a user-based installation and accessibility to corporate resources from anywhere at anytime. [< TOP >](#)

Yes, the product satisfied Ceer Consulting because of the following reasons:

- Ceer Consulting chose TEXAS Systems' SureWare B-Gate as a reliable, secure remote access solution that saved the company money in acquisition and maintenance costs, was easy to install and provided functionality that increased company productivity and decreased resource demands.
- SureWare B-Gate's SSL VPN appliance gives a higher return on investment than a traditional remote access system because its acquisition cost is significantly lower than an equivalent IPsec system and its maintenance costs are minimal.
- In addition to SureWare B-Gate's reliability and affordability, the virtual network offers flexibility in its services and accessibility to the corporate network.
- Since its installation, SureWare B-Gate has effectively and reliably handled all e-mail requirements for its remote staff. The new SSL VPN is excellent and the client install was easy.
- The B-Gate option was the best way to create an SSL connection from a client anywhere on the Internet back to our exchange server, a connection that is secure and can go anywhere.
- The TEXAS SureWare B-Gate solution has increased company productivity and reduced the demand for network storage because it allows the full use of the Outlook client.

Section C: Applied Theory

6. Pretty Good Privacy (PGP) consists of five services: authentication, confidentiality, compression, e-mail compatibility and segmentation. [< TOP >](#)

Summary of PGP Services

Function	Algorithms Used	Description
Digital signature	DSS/SHA or	A hash code of a message is created using SHA-1.
Message	CAST or IDEA or	A message is encrypted using CAST-128 or IDEA or
Compression	ZIP	A message may be compressed, for storage or

		transmission, using ZIP.
E-mail compatibility	Radix-64 conversion	To provide transparency for email applications, an encrypted message may be converted to an ASCII string using radix-64 conversion.
Segmentation	–	To accommodate maximum message size limitations, PGP performs segmentation and reassembly.

7. The threats can be divided into two categories: those that need a host program, and those that are independent. The former are essentially fragments of programs that cannot exist independently of some actual application program, utility, or system program. The latter are self-contained programs that can be scheduled and run by the operating system. [<](#)
[TOP](#)
[>](#)

We can also differentiate between those software threats that do not replicate and those that do. The former are fragments of programs that are to be activated when the host program is invoked to perform a specific function. The latter consist of either a program fragment (virus) or an independent program (worm, bacterium) that, when executed, may produce one or more copies of itself to be activated later on the same system or some other system.

Trapdoors

A trap door is a secret entry point into a program that allows someone that is aware of the trap door to gain access without going through the usual security access procedures. Trap doors have been used legitimately for many years by programmers to debug and test programs. This usually is done when the programmer is developing an application that has an authentication procedure, or a long setup, requiring the user to enter many different values to run the application. To debug the program, the developer may wish to gain special privileges or to avoid all the necessary setup and authentication. The programmer may also want to ensure that there is a method of activating the program should something be wrong with the authentication procedure that is being built into the application. The trap door is code that recognizes some special sequence of input or is triggered by being run from a certain user ID or by an unlikely sequence of events.

Trap doors become threats when they are used by unscrupulous programmers to gain unauthorized access. It is difficult to implement operating system controls for trap doors. Security measures must focus on the program development and software update activities.

Logic Bomb

One of the oldest types of program threat, predating viruses and worms, is the logic bomb. The logic bomb is code embedded in some legitimate program that is set to "explode" when certain conditions are met. Examples of conditions that can be used as triggers for a logic bomb are the presence or absence of certain files, a particular day of the week or date, or a particular user running the application. In one famous case, a logic bomb checked for a certain employee ID number (that of the bomb's author) and then triggered if the ID failed to appear in two consecutive payroll calculations. Once triggered, a bomb may alter or delete data or entire files, cause a machine halt, or do some other damage.

Trojan Horses

A Trojan horse is a useful, or apparently useful, program or command procedure containing hidden code that, when invoked, performs some unwanted or harmful function.

Trojan horse programs can be used to accomplish functions indirectly that an unauthorized user could not accomplish directly. For example, to gain access to the files of another user on a shared system, a user could create a Trojan horse program that, when executed, changed the invoking user's file permissions so that the files are readable by any user. The author could then induce users to run the program by placing it in a common directory and naming it such that it appears to be a useful utility. An example is a program that ostensibly produces a listing of the user's files in a desirable format. After another user has run the program, the author can then access the information in the user's files. An example of a Trojan horse program that would be difficult to detect is a compiler that has been modified to insert additional code into certain programs as they are compiled, such as a system login program. The code creates a trap door in the login program that permits the author to log on to the system using a special password. This Trojan horse can never be discovered by reading the source code of the login program.

Another common motivation for the Trojan horse is data destruction. The program appears to be performing a useful function (e.g., a calculator program), but it may also be quietly deleting the user's files.

Viruses

A virus is a program that can "infect" other programs by modifying them; the modification includes a

copy of the virus program, which can then go on to infect other programs.

Biological viruses are tiny scraps of genetic code-DNA or RNA-that can take over the machinery of a living cell and trick it into making thousands of flawless replicas of the original virus. Like its biological counterpart, a computer virus carries in its instructional code the recipe for making perfect copies of itself. Lodged in a host computer, the typical virus takes temporary control of the computer's disk operating system. Then, whenever the infected computer comes into contact with an uninfected piece of software, a fresh copy of the virus passes into the new program. Thus, the infection can be spread from computer to computer by unsuspecting users, who either swap disks or send programs to one another over a network. In a network environment, the ability to access applications and system services on other computers provides a perfect culture for the spread of a virus.

Worms

Network worm programs use network connections to spread from system to system. Once active within a system, a network worm can behave as a computer virus or bacteria, or it could implant Trojan horse programs or perform any number of disruptive or destructive actions.

To replicate itself, a network worm uses some sort of network vehicle. Examples include the following:

- **Electronic mail facility:** A worm mails a copy of itself to other systems.
- **Remote execution capability:** A worm executes a copy of itself on another system.
- **Remote login capability:** A worm logs onto a remote system as a user and then uses commands to copy itself from one system to the other.

The new copy of the worm program is then run on the remote system where, in addition to any functions that it performs at that system, it continues to spread in the same fashion.

A network worm exhibits the same characteristics as a computer virus: a dormant phase, a propagation phase, a triggering phase, and an execution phase. The propagation phase generally performs the following functions:

- i. Search for other systems to infect by examining host tables or similar repositories of remote system addresses.
- ii. Establish a connection with a remote system.
- iii. Copy itself to the remote system and cause the copy to be run.

The network worm may also attempt to determine whether a system has previously been infected before copying itself to the system. In a multiprogramming system, it may also disguise its presence by naming itself as a system process or using some other name that may not be noticed by a system operator.

As with viruses, network worms are difficult to counter. However, both network security and single-system security measures, if properly designed and implemented, minimize the threat of worms.

[< TOP OF THE DOCUMENT >](#)