**Unit-III: Authentication and Hash function**

**Session -1 Authentication requirements Date: 05.08.2013 Period: 03**

Introduction: Presentation (http://www.cise.ufl.edu/~nemo/crypto/stallings/ch11.ppt)

Remember by keywords: Requirement of Authentication functions

* disclosure
* traffic analysis
* masquerade
* content modification
* sequence modification
* timing modification
* source repudiation
* destination repudiation

**Conclusion:Quiz**

1. Define integrity and nonrepudiation?

Integrity:

Service that ensures that only authorized person able to modify the message.

Nonrepudiation:

This service helps to prove that the person who denies the transaction is true or false.

1. Define Disclosure

 Release of message contents to any person or process not processing the appropriate cryptographic key

1. What is meant by Traffic Analysis?

 Discovery of the pattern of traffic between parties. In a connection oriented application, the frequency and duration of connections could be determined. In either a connection oriented or connectionless environment, the number and length of messages between parties could be determined.

1. What is meant by Masquerade?

 Insertion of messages into the network from a fraudulent source. This includes the creation of messages by an opponent that are purported to come from an authorized entity. Also included are fraudulent acknowledgements of message receipt or no receipt by someone other than the message recipient.

1. What is meant by Content modification?

 Changes to the contents of a message , including insertion, deletion, transposition, and modification.

**Session -2 Authentication functions Date: 06.08.2013 Period: 01**

Recap: Group quiz

Activity Description: We can divide the learners into two teams and instruct each team to prepare 5 questions on the Feedback and its types. After 5 minutes of preparation, each team will ask the other team the questions prepared.

**Content: Message encryption**

Presentation (<http://www.cise.ufl.edu/~nemo/crypto/stallings/ch11.ppt> ) and

Recall by words:

Symmetric encryption,

Asymmetric encryption,

 Authentication,

 Digital signature,

Confidentiality,

Secrecy,

 Message encryption,

 Message Authentication Code and

 Hash function

**Conclusion:Quiz**

1. **Differentiate symmetric and asymmetric encryption?**

Symmetric It is a form of cryptosystem in which encryption and decryption performed usingthe same key. Eg: DES, AES

Asymmetric

It is a form of cryptosystem in which encryption and decryption Performed using two keys. Eg: RSA, ECC

1. **Define security mechanism**

It is process that is designed to detect prevent, recover from a security attack. Example: Encryption algorithm, Digital signature, Authentication protocols.

1. **What is message authentication?**

It is a procedure that verifies whether the received message comes from assigned source has not been altered. It uses message authentication codes, hash algorithms to authenticate the message.

1. **Define the classes of message authentication function.**

Message encryption: The entire cipher text would be used for authentication.

 Message Authentication Code: It is a function of message and secret key produce a fixed length value.

 Hash function: Some functions that map a message of any length to fixed length which serves as authentication.

**Session -3 Message Authentication Code (MAC) & Hash functions**

**Date: 06.08.2013 Period: 05**

* **Remember by Keywords**
* input message *M*
* MAC function *C*
* shared secret key *K*
* message authentication code MAC

**Content: Message authentication code**

Presentation (<http://www.cise.ufl.edu/~nemo/crypto/stallings/ch11.ppt> ) and board explanation

**Conclusion:Quiz**

1. **What you meant by MAC?**

MAC is Message Authentication Code. It is a function of message and secret key which produce a fixed length value called as MAC. MAC = Ck(M) Where M = variable length message. K = secret key shared by sender and receiver. CK(M) = fixed length authenticator.

1. **Differentiate internal and external error control.**

Internal error control: In internal error control, an error detecting code also known as frame check sequence or checksum.

External error control: In external error control, error detecting codes are appended after encryption.

1. **What is the meet in the middle attack?**

This is the cryptanalytic attack that attempts to find the value in each of the range and domain of the composition of two functions such that the forward mapping of one through the first function is the same as the inverse image of the other through the second function-quite literally meeting in the middle of the composed function.

**Session -4 Hash functions Date: 07.08.2013 Period: 02**

**Recap: Group Quiz**

Activity Description: We can divide the learners into two teams and instruct each team to prepare 5 questions on the Feedback and its types. After 5 minutes of preparation, each team will ask the other team the questions prepared.

**Content: Hash functions and Message digest**

**Presentation (http://www.cisa.umbc.edu/courses/cmsc/687/spring07/slides/ch12.ppt) and**

**Recall by words**

**Conclusion: Recall by words**

**Hash function,**

**Message Digest,**

**Compression function,**

 **Message inputs size and**

 **Hash code size**

**Session – 5 MD5 message Digest algorithm Date:12.08.2013 Period: 03**

**Introduction: Presentation with Power point presentation and Video**

[**www.youtube.com/watch?v=aLvwpJcOy6s**](http://www.youtube.com/watch?v=aLvwpJcOy6s)

**Board Activity: Ask any one learner write the output equation of ‘B’ Buffer**

****

* **Conclusion : Word puzzle (Quiz)**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| F | S | F | H | W | O | E | Y | L | I | H | N | X | I | T | B | F | C | M | T |
| O | R | I | O | Y | F | N | B | G | A | C | Y | F | V | O | K | X | A | I | M |
| U | N | V | E | Y | J | T | G | D | S | X | R | A | U | Y | W | P | T | E | P |
| R | X | E | L | S | V | I | D | N | V | B | E | B | T | M | P | B | V | F | S |
| A | Q | H | T | T | R | C | T | E | L | B | S | X | O | C | X | I | S | H | P |
| J | X | U | O | W | U | U | X | G | I | Q | B | P | A | H | Q | O | O | B | Y |
| W | B | N | T | V | E | Q | A | G | T | G | F | S | N | I | F | D | T | R | L |
| J | P | D | G | J | X | N | E | F | T | D | W | N | S | B | H | V | Q | F | M |
| W | C | R | F | S | V | N | T | X | L | H | R | D | D | W | G | D | G | T | T |
| A | N | E | Q | C | D | K | U | Y | E | I | D | O | P | Q | A | B | J | W | T |
| E | N | D | F | I | U | P | F | Y | E | B | T | I | M | T | X | S | K | U | O |
| N | G | A | A | V | O | A | Y | V | N | I | O | C | J | B | F | V | S | A | V |
| O | C | N | S | P | N | V | D | G | D | L | G | W | A | I | G | M | J | T | B |
| B | R | D | Y | Q | D | X | N | F | I | K | X | H | U | M | Q | A | Y | H | F |
| H | X | T | R | J | R | H | B | G | A | V | U | X | T | W | F | W | G | I | W |
| D | J | W | X | T | C | I | U | X | N | A | X | D | V | T | M | I | C | E | T |
| H | W | E | A | R | O | V | H | T | H | X | M | T | Y | D | J | R | T | D | V |
| N | J | L | V | J | N | T | B | A | H | V | Y | P | X | D | J | I | U | T | N |
| J | O | V | U | C | L | H | E | O | P | X | D | Y | M | L | S | O | H | H | O |
| U | D | E | I | F | P | O | N | K | R | E | Y | C | X | L | L | K | J | T | Q |

 |
|  |

* you store the most significant byte in the smallest address
* you store the *least* significant byte in the smallest address.
* What is the size of input
* How many rounds the compression function is compressed of

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| F | S | F | H | W | O | E | Y | L | I | H | N | X | I | T | B | F | C | M | T |
| O | R | I | O | Y | F | N | B | G | A | C | Y | F | V | O | K | X | A | I | M |
| U | N | V | E | Y | J | T | G | D | S | X | R | A | U | Y | W | P | T | E | P |
| R | X | E | L | S | V | I | D | N | V | B | E | B | T | M | P | B  | V | F | S |
| A | Q | H | T | T | R | C | T | E | L | B | S | X | O | C | B | V | F | H | P |
| J | X | U | O | W | U | U | X | G | I | Q | B | P | A | H | Q | O | O | B | Y |
| W | B | N | T | V | E | Q | A | G | T | G | F | S | N | I | F | D | T | R | L |
| J | P | D | G | J | X | N | E | F | T | D | W | N | S | B | H | V | Q | F | M |
| W | C | R | F | S | V | N | T | X | L | H | R | D | D | W | G | D | G | T | T |
| A | N | E | Q | C | D | K | U | Y | E | I | D | O | P | Q | A | B | J | W | T |
| E | N | D | F | I | U | P | F | Y | E | B | T | I | M | T | X | S | K | U | O |
| N | G | A | A | V | O | A | Y | V | N | I | O | C | J | B | F | V | S | A | V |
| O | C | N | S | P | N | V | D | G | D | L | G | W | A | I | G | M | J | T | B |
| B | R | D | Y | Q | D | X | N | F | I | K | X | H | U | M | Q | A | Y | H | F |
| H | X | T | R | J | R | H | B | G | A | V | U | X | T | W | F | W | G | I | W |
| D | J | W | X | T | C | I | U | X | N | A | X | D | V | T | M | I | C | E | T |
| H | W | E | A | R | O | V | H | T | H | X | M | T | Y | D | J | R | T | D | V |
| N | J | L | V | J | N | T | B | A | H | V | Y | P | X | D | J | I | U | T | N |
| J | O | V | U | C | L | H | E | O | P | X | D | Y | M | L | S | O | H | H | O |
| U | D | E | I | F | P | O | N | K | R | E | Y | C | X | L | L | K | J | T | Q |

**Session -6 Secure Hash Algorithm (SHA) Date: 13.08.2013 Period: 01**

**Content: Presentation with Power point presentation and Video**

* **Video: http://www.youtube.com/watch?v=aLvwpJcOy6s**

**Board Activity: Ask any one learner write the output equation of ‘A’ Buffer**

****

Conclusion : Quiz

1. How many bits are stored in MD buffer?

160 bits

1. SHA-1 use little endian or big endian architecture?

Big endian architecture

1. Tell any two revised SHA standard?

SHA-256, SHA – 384

**Session -7 Comparison of SHA-1 and MD5 Date:13.08.2013 period:05**

Recap: Quiz (crossword)



Content: power point presentation ( Key points of SHA-1 and MD-5 Hash algorithm)

Conclusion:

* **Remember by keywords**
* Security against brute force attack
* Security against cryptanalysis
* Speed
* Simplicity and compactness

Little Endian Vs Big Endian

**Session -8 RIPEMD Date:17.08.2013 Period: 03**

Content: Power point Presentation (www.cisa.umbc.edu/courses/cmsc/687/spring07/slides/ch12.ppt)

Conclusion:

* **Remember by keywords**
* Append Padding bits
* Append length
* MD buffer registers
* Compression function

**Session -9 HMAC & Digital signatures Date: 17.08.2013 Period: 07**

Content: Presentation slides ([www.eecis.udel.edu/~mills/teaching/eleg867b/crypto\_slides/ch13.ppt](http://www.eecis.udel.edu/~mills/teaching/eleg867b/crypto_slides/ch13.ppt) and www.cisa.umbc.edu/courses/cmsc/687/spring07/slides/ch12.ppt)

Conclusion: Questions and answers

1. **Distinguish between direct and arbitrated digital signature?**

The direct digital signature involves only the communicating parties.

The arbiter plays a sensitive and crucial role in this digital signature.

2. **What requirements should a digital signature scheme should satisfy?**

The signature must be bit pattern that depends on the message being signed.

The signature must use some information unique to the sender, to prevent both forgery and denial.

It must be relatively easy to produce the digital signature.

It must be relatively easy to recognize and verify the digital signature.

**3.What are the properties a digital signature should have?**

 **i)**It must verify the author and the data and time of signature.

ii)It must authenticate the contents at the time of signature.

iii)It must be verifiable by third parties to resolve disputes.