Quiz

Q1. Message Integrity ensures that only the sender and the receiver understands the content of the message. True or False?

Q2. End point authentication ensures that only the sender and the receiver understands the content of the message. True or False?

Q3. The aim of encryption is to hide the plain text as well as the encryption algorithm from intruders. True or False?

Q4. Symmetric key encryption uses identical keys at both the communicating parties. True or False?

Q5. We use Cipher Block Chaining (CBC) to

a. Reduce the overhead associated with sending random bits along with cipher text

b. Make the encryption more secure

c. Hide the random bits used in the process of encryption

d. None of the above

Q6. An attacker launching brute force attack on an N-bit block cipher in the worst case will have to try out how many combinations?

a. 2^N

b. N!

c. (2^N)!

d. (N!)^2

Q7. AES is an example of

a. Symmetric key cryptography

b. Public key cryptography

c. Hybrid key cryptography

d. None of the above

Q8. Suppose Alice is using public key cryptography whereby Alice uses Bob's public key to encrypt her messages for Bob. What is being achieved?

a. Message Integrity

b. Sender Authentication

c. Both a and b

c. None of above

Q9. If you want to send only a short message to your peer, what type of encryption technique would be more efficient?

a. Symmetric key cryptography with an appropriate key exchange mechanism

b. Public key cryptography

c. Hybrid key cryptography

d. None of the above

Q10. A digital signature provides

a. Confidentiality

b. Message integrity & Non-repudiation

c. Message integrity only

d. None of the above

Q11. What is the job of a Certification Authority (CA) in Public Key Infrastructure (PKI)?

a. Maintain private keys of all authenticated users

b. Guarantee that the public key of the registered user is authenticated by issuing a digital certificate

c. Issues a session key to both end parties for communication

d. CA's are not used in PKI

Q12. The secure email system of Figure 8.21 in text provides sender as well as receiver authentication. True or False?

Q13. Suppose Bob wants to send Alice a digital signature for the message m. To create the digital signature

a. Bob applies a hash function to m and encrypts the result with his public key

b. Bob applies a hash function to m and encrypts the result with Alice's public key

c. Bob applies a hash function to m and encrypts the result with Alice's private key

d. Bob applies a hash function to m and encrypts the result with his private key

Resource created 4 months ago (Wednesday 04 September 2019, 06:45:28 PM), last modified about a month ago (Friday 15 November 2019, 02:55:29 PM).

Comments

(/COMP3331/19T3/forums/search?forum_choice=resource/31927)

(/COMP3331/19T3/forums/resource/31927)

Add a comment

Xianlei Wang (/users/z5182667) about a month ago (Sun Nov 24 2019 14:26:31 GMT+0800 (中国标准时间))

For Q3,why it is false?

for q5,I think b is also right

For q9,why it is b,the Ks is more quick than the K（pub） and K(pri)

For Q10,why it is B,I think the digital signature can provide Non-repudiation with the CA,only digital sinature can be used by others.it can only provide Message integrity.And other textbook also say the digital signature can provide integrity

Reply

Salil Kanhere (/users/z3116703) about a month ago (Sun Nov 24 2019 17:51:52 GMT+0800 (中国标准时间))

Q3. Encryption algorithms are known to everyone. The key is what makes the ciphertext undecipherable to those who do not have it.

Q5. I would say a is a better answer. CBC addresses the issue of ensuring that the same plaintext (if encountered multiple times) does not map to the same ciphertext. So as such it is not necessarily improving the encryption algorithm itself. At the very high level, one could use that argument as a broad brush but a is certainly more specific

Q9.Yes but there is an overhead to setup the shared key in the first place, which will rely on public key crypto. And if the message is short then it comparable to the length of the shared key that would need to be exchanged using public key crypto.

Q10. Digital signatures also provide non-repudiation. Assume Bob is sending a digitally signed message to Alice. Since the message received by Alice has Bob's signature (which she can verify using his public key), she can be sure that the message was sent by Bob and no one other than Bob, since only Bob can have Bob's private key.

Reply

Matthew Immanuel (/users/z5187551) 27 days ago (Tue Dec 03 2019 11:07:42 GMT+0800 (中国标准时间))

Is it also correct to assume that digital signature provides authentication? So Digital signature provides authentication, integrity and non repudiation

Reply

Salil Kanhere (/users/z3116703) 27 days ago (Tue Dec 03 2019 11:18:09 GMT+0800 (中国标准时间))

see - https://webcms3.cse.unsw.edu.au/COMP3331/19T3/forums/2751260 (https://webcms3.cse.unsw.edu.au/COMP3331/19T3/forums/2751260)

Reply

Saloni Goda (/users/z5215272) about a month ago (Fri Nov 29 2019 19:36:44 GMT+0800 (中国标准时间))

For q9, isn't there overhead to share public key as well?

Reply

Salil Kanhere (/users/z3116703) about a month ago (Fri Nov 29 2019 23:03:53 GMT+0800 (中国标准时间)), last modified about a month ago (Fri Nov 29 2019 23:04:41 GMT+0800 (中国标准时间))

There is no computational overhead involved. Sure there is some overhead for transmitting it but they key is only a few bits lon

Reply

Xianlei Wang (/users/z5182667) about a month ago (Sun Nov 24 2019 18:16:44 GMT+0800 (中国标准时间))

for q10,but if bob private key is lost,and others can use bob's public key,others can prentend as bob to send infomation,by using bob's private key to encrypt with m in hash function,and send bob public key ,Kpri(H(m)),m I think only in the situation that CA encrypt the bob public key can avoid it

Reply

Salil Kanhere (/users/z3116703) about a month ago (Sun Nov 24 2019 18:25:10 GMT+0800 (中国标准时间)), last modified about a month ago (Sun Nov 24 2019 18:26:33 GMT+0800 (中国标准时间))

The basic assumption with all crypto discussions is that keys are never lost or stolen. And yes having a key certified by a CA could potentially protect against key theft. Having a CA also allows someone to revoke an older key if it every gets lost or stolen.

Reply

Xianlei Wang (/users/z5182667) about a month ago (Mon Nov 25 2019 14:50:52 GMT+0800 (中国标准时间))

so if do the similar question after，we assume keys are never lost or stolen ?

Reply

Salil Kanhere (/users/z3116703) about a month ago (Mon Nov 25 2019 17:53:23 GMT+0800 (中国标准时间))

yes, unless specifically noted/implied in the question.

Reply

Nadeem Ahmed (/users/z3003139) about a month ago (Fri Nov 22 2019 13:51:07 GMT+0800 (中国标准时间))

Solution:

1. False

2. False

3. False

4. True

5. a

6. c

7. a

8. d

9. b

10. b

11. b

12. True

13. d

Reply

Chinmay Manchanda (/users/z5216191) about a month ago (Thu Nov 28 2019 11:37:09 GMT+0800 (中国标准时间))

if we use d), won't it allow anyone with Bob's public key to access it ?.
Maybe B's the right answer

Thanks.

Reply

Salil Kanhere (/users/z3116703) about a month ago (Thu Nov 28 2019 17:04:01 GMT+0800 (中国标准时间))

I presume you mean question 13. The point here is for Bob to be able to prove that he signed the message and no one else. So d is the correct answer as only Bob can be in possession of his private key, which is confirmed by applying his public key to the signature. The goal here is not to encrypt the message.

Reply

Xianlei Wang (/users/z5182667) about a month ago (Mon Nov 18 2019 17:21:19 GMT+0800 (中国标准时间))

Q1：false

Q2：False

Q3：False

Q4：True

Q5：B

Q6:A(?

Q7:A

Q8：D

Q9：A

Q10：C

Q11：B

Q12：which figure

Q13:B/D

Reply