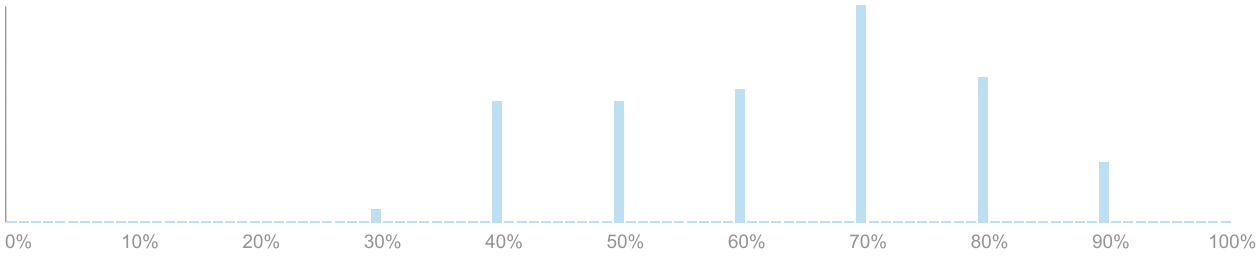
Quiz Summary

Section Filter

Student analysis (https://canvas.nus.edu.sg/files/861475/download?download_frd=1&verifier=tDEA8SEt3yuHNBlKrvD321m5z5J8mR5ZggcdBl01)

Item analysis

Average score	High score	Low score	Standard deviation	Average time
64%	90%	30%	1.55	26:43



Question Breakdown

Attempts: 67 out of 67

Which of the following statements is TRUE about the principles/concepts in information security?

+0.32

Discrimination Index

Confidentiality implies integrity.	0 %

Data authentication implies integrity and confidentiality of data.	3 respondents	4 %
(D)DoS attack aims at deteriorating availability.	62 respondents	**93 %**
Authentication ensures non-repudiation.	1 respondent	1 %
None of the above.	1 respondent	1 %

93%
answered
correctly

Attempts: 67 out of 67

Which of the following statement is WRONG about symmetric crypto schemes?

+0.38

Discrimination Index

Stream cipher is secure if random keystream is never reused.	9 respondents	13 %
A receiver of message encrypted with symmetric crypto scheme can convince a third person (not sender) that the message is originated from the sender.	48 respondents	**72 %**
Successful decryption of a received ciphertext does not necessarily imply the integrity of the plaintext.	1 respondent	1 %
When designing authenticated encryption, Encrypt-then-MAC is the first option to consider.	3 respondents	4 %
None of the above.	6 respondents	9 %

72%
answered
correctly

Attempts: 67 out of 67

In the CBC mode of encryption, it is important how to select IV (initialization vector). Which of the following way is considered as a good way to choose IV?

+0.49

Discrimination Index

Hash value of the current timestamp	1 respondent	1 %
Pseudo random number generated by a publicly-known pseudo random number generator with the current timestamp as a seed	14 respondents	21 %
Hash value of a secret key K and the current timestamp	38 respondents	**57 %**
Pseudo random number generated with a (static) user-entered password P	4 respondents	6 %
None of the above.	10 respondents	15 %

57% answered correctly

Attempts: 67 out of 67

Which of the following statements is WRONG about CTR mode?

+0.45

Discrimination Index

CTR mode can provide semantic security.		0 %
CTR mode is secure as long as counters are not repeated or reused.	8 respondents	12 %
CTR mode is not secure when the IV (i.e., X1) is predictable.	53 respondents	**79 %**

In CTR mode encryption and decryption, processing of multiple blocks is parallelizable.		0 %
CTR mode does not ensure integrity.	6 respondents	9 %

79%
answered
correctly

Attempts: 67 out of 67

Which of the following statements is CORRECT about message authentication in symmetric crypto schemes?

+0.38

Discrimination Index ⓘ

CBC encryption and CBC MAC calculation must be done separately.	21 respondents	**31 %** ✓
CBC mode encryption allows manipulation (e.g. flipping) of any targeted bit in all plaintext blocks in a meaningful way.	15 respondents	22 %
As long as one-time pad is generated correctly, stream cipher offers authentication.	8 respondents	12 %
As long as we use Encrypt-then-MAC authenticated encryption, ECB mode encryption offers semantic security.	7 respondents	10 %
None of the above.	16 respondents	24 %

31%
answered
correctly

Attempts: 67 out of 67

Which of the following statements is CORRECT about asymmetric crypto scheme?

+0.42

Discrimination Index

Encryption should be done with the public key of the sender.	2 respondents	3 %
Digital signature should be made with the sender's private key.	51 respondents	**76 %**
DH key agreement protocol is used for encryption and digital signature.	4 respondents	6 %
The security of RSA algorithm relies on difficulty of Discrete Logarithm Problem.	6 respondents	9 %
None of the above.	4 respondents	6 %

76% answered correctly

Attempts: 67 out of 67

Which of the following statements is WRONG about public key infrastructure?

+0.5

Discrimination Index

PKI is important to prevent impersonation or man-in-the-middle attacks under asymmetric crypto schemes.	11 respondents	16 %
Revocation of certificates is one of the responsibilities of CA.		0 %
The public key of the CA must be trusted by all entities involved.	7 respondents	10 %

Digital certificate is signed by a trusted CA to endorse the mapping between an entity's identity and the CA's public key.	23 respondents	**34 %**	✓
None of the above.	26 respondents	39 %	

34%
answered
correctly

Attempts: 67 out of 67

Which of the following is NOT a security property required for cryptograhic (secure) hash functions?

-0

Discrimination
Index ⓘ

Semantic security	67 respondents	**100 %**	✓
Collision resistance		0 %	
Preimage resistance		0 %	
Second preimage resistance		0 %	
None of the above.		0 %	

100%
answered
correctly

Attempts: 66 out of 67

Which of the following statements is WRONG about attack complexity against a cryptographic hash function H that outputs 256-bit digest? Assume the best attack is random search as done in the lecture.

+0.44

Discrimination Index

Given a certain data X, finding another data (X') that generates the same digest H(X) requires an attacker on average 2^{255} trials.	1 respondent	1 %
Finding collision (any 2 different data X and X' that generate the same digest) takes on average 2^{255} trials.	54 respondents	**81 %**
Given a certain digest Y, which is calcualted from a certain input data X, finding another data X' that generates digest Y takes on average 2^{255} trials.	2 respondents	3 %
Birthday paradox affects attack complexity of all security properties required for cryptographic hash functions.	8 respondents	12 %
None of the above.	1 respondent	1 %
No Answer	1 respondent	1 %

81% answered correctly

Attempts: 66 out of 67

Which of the following statement is CORRECT about one-way hash chain and its application?

+0.27

Discrimination Index

Among the security properties of cryptographic hash functions, collision resistance is the most crucial for the hash chain to be secure.	14 respondents	21 %

Hash chain is to be used in the same order	10 respondents	15 %	
In S/Key, the number of hash calculation that the server needs to perform is increasing as authentication rounds progress.	15 respondents	22 %	
In S/Key, the number of hash calculation at the client side is increasing as authentication rounds progress.	18 respondents	27 %	
None of the above.	9 respondents	**13 %**	✓
No Answer	1 respondent	1 %	

13%
answered
correctly