Section-A: Repeated Questions

1. How can you break a substitution cipher? Specify your answer with an example.

Years: 2012, 2016, 2019

2. What is the purpose of an S-box? Give an example of a bad S-box.

Years: 2011, 2019

3. The figure shown in Fig.3(b) is called the cascade of NMAC (nested MAC). Is this construction of NMAC secure?

Years: 2012, 2016, 2019

4. Define message authentication code (MAC). What is the significance of MAC? "Integrity requires a key" — explain.

Years: 2010, 2011, 2013, 2019

5. Compare AES to DES. For each of the following elements of DES, indicate the comparable element in AES or explain why it is not needed in AES:

i) XOR of subkey with the input to the f function
ii) f function
iii) Permutation P
iv) Swapping of halves of the block
v) XOR of the f function with the left half of the block
Years: 2017, 2019

6. Suppose Alice and Bob wish to do Diffie-Hellman key exchange… Show the intermediate quantities… Final shared secret…

And:

Unknown to Alice and Bob, Eve is listening and can inject her own texts. Explain how Eve can use e to perform a MITM attack.

Years: 2010, 2017, 2018, 201

7. Define birthday paradox and secure PRG. How does secure PRG help to make OTP practical?

Years: 2012, 2014, 2018, 2019

8. What can we infer from Shannon's definition of perfect secrecy? Is one-time-pad (OTP) perfect secrecy? Justify your answer.

Years: 2010, 2012, 2013, 2014

9. Mention the distinguishing properties of digital signature. Explain the digital signature process without encryption.

Years: 2011, 2012, 2016, 2019

10. What is MAC? Briefly explain the construction of CBC-MAC and NMAC.

Years: 2011, 2013, 2014, 2017, 2019

11. Describe the following forms of typical attacks:

i) Ciphertext-only attack

ii) Known-plaintext attack

iii) Chosen-plaintext attack

iv) Chosen-ciphertext attack

Years: 2013, 2014, 2017

12. Briefly explain AES encryption and decryption technique. / Describe entirely how the AES crypto system works.

Years: 2011, 2014, 2017, 2019

13. How can you prove that security does increase by double encryption, but it does not increase much? Explain with a possible attack scenario.

Also appears as: Show attacks on: Double-DES
Years: 2013, 2014, 2019

14. What is textbook RSA? Why is it not secure? Explain. / Show attacks on textbook RSA.

Years: 2013, 2014, 2018

15. "PRG must be unpredictable." Explain.

Years: 2012, 2014, 2017

16. For ECBC MAC… after how many messages must the key be changed? (bound calculation)

Years: 2017, 2018

Section-B: Repeated Questions (Security, Systems, Ethics, etc.)

1. Write down the concept of SQL injection with an example. / with two different examples.

Years: 2013, 2016, 2019

2. What is Firewall? What is the purpose of port scanning?

Years: 2016, 2017, 2019

3. What are DoS and DDoS attacks? How are these types of attacks launched?

Years: 2010, 2016, 2019

4. Explain Bell-LaPadula confidentiality model with proper example.

Years: 2012, 2016, 2017, 2019

5. What makes an Operating System secure or trustworthy? Describe various features of trusted Operating Systems. / What is a trusted system?

Years: 2012, 2013, 2014, 2016, 2019

6. Write a short note on the famous Enigma machine.

Years: 2011, 2012, 2013, 2014, 2016

7. "Anything that can be done with trusted authority can also be done without." — Explain in the context of Blockchain.

Years: 2010, 2016
(Also repeated in blockchain immutability + consensus explanation — 2017, 2019)

8. Explain the function and procedure of digital signature. / Draw and describe the process of creating and verifying digital signatures.

Years: 2016, 2019

9. What is malicious code? Describe five types or properties.

Years: 2012, 2013, 2014

10. Case Study (Ethical):

- Gautam publishes without supervisor's name

- Rizwan leaks names to researcher
  Years: 2016, 2019

11. Describe briefly “lattice model of security” and “Bell-LaPadula confidentiality model”.

Years: 2012, 2016, 2017

12. What is a trusted system? Write down the security features of a trusted system.

Years: 2012, 2013, 2014

13. Explain the inference problem of database security. Give examples of indirect attacks.

Years: 2012, 2013

14. What do you mean by ‘no eavesdropping’ and ‘no tampering’? How can we ensure them in secure communication?

Years: 2010, 2018