Charotar University of Science and Technology

Devang Patel Institute of Advance Technology and Research

Department of Computer Science & Engineering

Academic Year: 2021-22 [6th Semester]

CS345 Cryptography and Network Security Assignment

1. Calculate the cipher text for the following scenarios.

Sr. No.	Plaintext	Key	Algorithm
1.	attack is today	13	Additive
2.	we live in insecure world	13	Multiplicative
3.	this is an assignment	15,20	Affine
4.	welcome to the world of cryptography	7	Shift cipher
5.	how was the attack	10	Autokey
6.	hope you are safe and sound	covid	Vigenere
7.	check your internet connectivity	covid	Playfair
8.	be ready for the examination	backup	Hill cipher
9.	transposition ciphers are vulnerable to several kinds of cipher text only attacks	eight	Columner
10.	meet me at tajmahal on the valentine day	Rows=4	Railfence

2. Calculate the plaintext for the following scenario.

Sr. No.	Plaintext	Key	Algorithm
1.	JXUCQDMXEXQISEDVYTUDSUYDXYCIUBVWQYDIJXUSEDVYTUDSUEVEJXUHI	13	Additive
2.	VQEVFQKPEADQIDAJSQNECYPLELPGNOLPQSIANIPANYQLPQKEDFZADQLPQENQUKPEZE	17	Multiplicative
3.	FZAPEPSDJZCDTOJCLDTRCDRPCKSRDMCJOJFB	7,15	Affine
4.	MAXIXLLBFBLMLXXLWBYYBVNEMRBGXOXKRHIIHKMNGBMRMAXHIMBFBLMLXXLHIIHKMNGBMRBGXOXKRWBYYBVNEMR	19	Shift cipher
5.	GHCZEHRHGQRHEUNHYOCYUNHAMTBKCLWJ	N	Autokey
6.	CYKTWOHRDPOKEQDOEWWVDOVEDUUIAK	ahmedabad	Vigenere

7.	LAZSMCYFTQHEIMFCPVCSLAXV	covid	Playfair
8.	BAPHYFJIXGGCHZHMYZ	backup	Hill cipher
9.	GUIEVSHLOIEIEIYCWTIMYFRNRTOLKIRSCEP ADKAOEFEEWUOENLPTRETIL	insert	Columner
10.	SIAIERAENEYSYSTTFIEAGDROIGCTMLUSIIS HDNVURHUIOTPROLETAIETNTRSENIRNO	Rows=5	Railfence

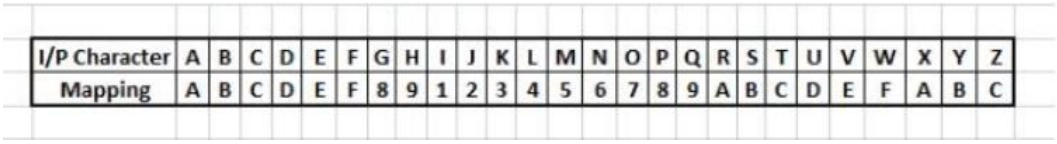
3. Perform the appropriate attack on the following scenarios. Also fill up the '?' marks in given table. (Show the steps for each calculation)

Sr. No.	Plaintext	Ciphertext	algorithm	Key	Attack	Remark
1.	yes	CIW	Shift cipher	?	?	Ciphertext = XVIEWYWI. Find the plaintext.
2.	?	NCJAEZRCLASJLYODE PRLYZRCLASJLCPEHZ DTOPDZQLNZTY	Additive cipher	?	?	-
3.	ab	GL	Affine	?	?	Ciphertext = XPALASXYF GFUKPXUSO GEUTKCDGF XANMGNVS. Find the plaintext.

4. Use the Playfair Cipher to encrypt the given plain text using key="cryptography". Here, calculate plaintext using your ID and Full name. For ex: If your id is 19dce001 and name is ABC XYZ, your plaintext will be: 19dce001abcxyz
5. Use the Hill Cipher to encrypt the plain text using key=backup. Here, calculate plaintext using your ID and Full name. For ex: If your id is 19dce001 and name is ABC XYZ, Your plaintext will be : 19dce001abcxyz.
6. Find the multiplicative inverse of 132 and 80 in Zp. Here Calculate P using your ID. For example: your ID is 17dcs025 so P=17+25=42. So, here P=42.
7. Calculate the number of possible keys for affine cipher for Zp. Here, Calculate P using your ID. For example: your ID is 17dcs025 so P = 17+25 = 42.
8. Encrypt and Decrypt the text with the help of key pair (7, 2) using affine cipher. Here, the plain text will be your ID + your name + surname **(size of Plaintext must be 15 characters. for example, your ID and name is 20DCS001 and Vidhi Pandya then plaintext will be 20DCS001vidhipa as it reaches the limit of PT)**.
   Also give the proof through an example having the same plain text for the below stated two statements.
   (1) Additive cipher is special case of affine cipher

(2) Multiplicative cipher is special case of affine cipher.

9. Find the K1 and K2 using SDES using the given key K. Here calculate the K using your Id. For Example your ID is 17dcs005 then K will be binary of 17005. Take first 10 bits of your binary as K.
10. Find out the first round key using DES algorithm. The key with parity bit will be generated by your name + middle name + surname (size of key should be 16 characters). Mapping of characters to convert input in to hexadecimal form is shown in the image (Note : if your name is very short and not having 16 characters then you need to repeat your name to create 16 character key)



I/P Character	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Mapping	A	B	C	D	E	F	8	9	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	A	B	C

11. The encryption algorithm to be used is RSA. Given two prime numbers 11 and 3 and public key (e) is 3. Calculate the decryption key and calculate the ciphertext if the given plaintext is 7.
12. Elaborate various kinds of attacks on RSA algorithm.
13. Compare public key and private key cryptography. Also list various algorithms for each
14. Briefly explain the model of Asymmetric Cryptosystem.
15. Explain RSA algorithm and list the possible approaches to attacking it.
16. Describe MD5 message digest algorithm.
17. What characteristics are needed in a secure hash function?
18. Write the properties of hash functions.
19. Explain SHA512 Algorithm.
20. What characteristics are needed in a secure hash function?
21. What is MAC? Explain HMAC.
22. How following can be achieved with message authentication: Message authentication, Message authentication and confidentiality
23. How message authentication code can be used to achieve message authentication and confidentiality
24. What is digital signature? Explain its use with the help of example.
25. List the security services provided by digital signature. Write and explain the Digital Signature Algorithm.
26. Explain key distribution using KDC.
27. In symmetric encryption, describe the ways in which key distribution can be achieved between two parties A and B?
28. What is the purpose of X.509 standard?
29. Which techniques are used for the distribution of public keys?
30. Explain Key Distribution methods.
31. List and explain various key management techniques.
32. Discus the ways in which public keys can be distributed to two communication parties.

33. Explain authentication mechanism of Kerberos.
34. What four requirements were defined for Kerberos?
35. Explain Kerberos Authentication System
36. What problem was Kerberos designed to address?
37. Briefly explain how session key is distributed in Kerberos.
38. Write a short note on SSL.
39. Define – SSL session and SSL connection.
40. Which parameters are used to define SSL state and SSL connection?
41. Define SSL session and SSL connection. Which parameters define session state and connection state?
42. Explain Secure Socket Layer Protocol
43. How can we achieve web security? Explain with example.
44. List and define the parameters that define secure socket layer connection state.
45. Explain Rabin Crypto System with example.
46. Explain Elgamal Cryptosystem with example.

Due Date for Submission: 25/2/2022

Note:

All the students must have knowledge regarding the above mentioned questions.

You need to write the assignment in a notebook.

Batch A Students will write the answers of following questions

Q-1 (1, 4, 7, 10), Q-2 (2, 5, 8), Q-3 (1), 4, 7, 10, 12, 23, 30, 42

Batch B Students will write the answers of following questions

Q-1 (2, 5, 8), Q-2 (1, 4, 9), Q-3 (2), 5, 8, 11, 16, 22, 28, 34, 40

Batch C & D Students will write the answers of following questions

Q-1 (3, 6, 9), Q-2 (3, 6, 7, 10), Q-3 (3), 6, 9, 15, 19, 28, 36, 46