Admission No:

Department of Computer Science and Engineering, SVNIT, Surat
B.Tech. III – Semester 6, Global Elective Course – Cryptography (CS362)
Date: 25th April, 2022 Total Marks: 20 Marks

1.	Find the last digit of 7^{2013} mod 10.				Ans
	(a) 4 mod 10	(b) 1 mod 10	[✓ (c) 7 mod 10]	(d) 2013 mod 10	
2.	Find 29^{25} mod 11				
	(a) 1 mod 11	[✓ (b) 10 mod 11]	(c) 27 mod 11	(d) 7 mod 11	
3.	Which of the following is the functionality provided by Digital Signature but not by Message Authentication Code ?				
	(a) Authentication	(b) Integrity	[✓ (c) Non-repudiation]	(d) Availability	
4.	Find $2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60}$ mod 7.				
	(a) 1 mod 7	(b) 5 mod 7	[✓ (c) 0 mod 7]	(d) 6 mod 7	
5.	The one-time pad is susceptible to				
	(a) known plaintext attack	(b) known ciphertext attack	(c) chosen plaintext attack	[✓ (d) none of these]	
6.	Which of the following is/are invalid size for a finite field?				
	[✓ (a) 100]	(b) 89	(c) 289	(d) 133	
7.	Which of the following is synonymous with "hash of a message"?				
	(a) digital signature over a message	[✓ (b) message digest]	(c) message authentication code	(d) all of the above	
8.	The relation between the RSA encryption and decryption keys is				
	(a) $ed \equiv 1(mod\ n)$	[✓ (b) $ed \equiv 1(mod\ \emptyset(n))$]	(c) $ed \equiv 0(mod\ n)$	(d) $ed \equiv 0(mod\ \emptyset(n))$	
9.	In the following mode of operation, a single bit error in transmission may cause many bit errors in that block but no errors in subsequent blocks				
	(a) CFB mode	(b) CBC mode	[✓ (c) ECB mode]	(d) all of the above	
10.	The principal advantage of public key cryptography over secret key cryptography is				
	(a) simplified key management	(b) lower chip area	(c) improved speed	[✓ (d) higher security]	
11.	Birthday attack can be prevented by,				
	(a) using non-cryptographic hash function	[✓ (b) using larger hash value]	(c) using padding	(d) using smaller hash value	
12.	The ratio of "Time to encrypt a 10 KB message with 56-bit DES" to "Time to compute hash of a 10KB message with SHA-1" is				
	[✓ (a)>1]	(b)<1	(c)=1	(d)=0	
13.	The man-in-the-middle attack in Diffie-Hellman key agreement protocol can be solved using,				
	(a) encrypted communication	[✓ (b) authenticated communication]	(c) hash function	(d) all of the above	
14.	If an efficient algorithm for computing integer factorization is discovered, which of the following schemes will be no more secure?				
	(a) Diffie-Hellman	(b) Elgamal	[✓ (c) RSA]	(d) Both a and b	
15.	When hash function is used in Digital Signature, a hash is encrypted using				
	(a) Public key	[✓ (b) Private key]	(c) Shared secret key	(d) One time password	
16.	Following can be implemented using hash functions:				
	(a) Pseudo random number generator	(b) digital signature	(c) One-time password generator	[✓ (d) All of the above]	
17.	The elliptic curve is defined over finite field F_{17}, with coefficient values A=3 and B=8. What is the value of 3P if point P is (13, 0), the value of 3P is,				
	[✓ (a) (13,0)]	(b) Point at infinity	(c) (39,0)	(d) undefined	
18.	Two 8-bit words can be multiplied in $GF(2^8)$ by using irreducible polynomial of				
	[✓ (a) degree 7]	(b) degree 8	(c) degree 2^8	(d) none of the above	
19.	Cryptographic hash function can be constructed using,				
	(a) One way trapdoor function	(b) trapdoor function	[✓ (c) one way function]	(d) encryption function	
20.	Public key cryptography can be constructed using,				
	[✓ (a) One way trapdoor function]	(b) trapdoor function	(c) one way function	(d) encryption function	