Indian Institute of Engineering Science and Technology, Shibpur

B.Tech (IT) 7th Semester End Semester Examinations, 2022
Information and Systems Security (IT-4101)

Full Marks: 50 **Time: 3 Hours**

Attempt ANY FIVE questions

1. (a) State the RSA parameters generation algorithm. How are the parameters used for encryption and decryption?
(b) Prove that the possibility of factorization of large numbers will compromise the security of RSA encryption.

[5×2=10]

2. (a) Describe the idea of the Markle-Damgard scheme and explain why this idea is important for the design of a cryptographic hash function?
(b) Suppose a person uses RSA to digitally sign a document D where he actually signs the MD4 digest of D, and not D itself. Given: $|D| < 448$. Justify how the MD4 digest helps to make this system more secure against "chosen message attack", as compared to another system, whereby D itself is digitally signed using RSA, without the involvement of any hash function.

[5×2=10]

3. Using the RSA digital signature scheme, where p=809, q=751, and d=23, do the following:
(i) Calculate the public key e.
(ii) Sign and verify the message M1 = 100. Call the signature S1.
(iii) Sign and verify the message with M2 = 50. Call the signature S2.
(iv) Show that if M = M1×M2 = 5000, then S = S1×S2.

[10]

4. (a) Prove the following w.r.t. Cipher Block Chaining (CBC) mode of modern block ciphers, with the help of a diagram:
"A single bit error in ciphertext block C(j) during transmission is propagated to a single bit in plaintext block P(j+1) but multiple bits in P(j), at the decryption site."
(b) Encrypt the text "meetatfour" using Playfair cipher with the following secret key:

L	G	D	B	A
Q	M	H	E	C
U	R	N	I	F
X	V	S	O	K
Z	Y	W	T	P

Is the above cipher a monoalphabetic or polyalphabetic cipher? Why?

[5×2=10]

5. Prove that, given hash length of 2^n bits, the minimum number of queries (q) required to succeed in preimage attack against a cryptographic hash function with a success probability of at least ½ is approximately 0.69×2^n.

[10]

6. Prove that, given hash length of 2^n bits, the minimum number of queries (q) required to succeed in collision attack against a cryptographic hash function with a success probability of at least ½ is approximately $O(2^{n/2})$.

[10]

****