বাংলাদেশ ইউনিভার্সিটি অব প্রফেশনালস্

সেকশন/গ্রুপ Section - B

ইনভিজিলেটরের স্বাক্ষর

মোট পৃষ্ঠা সংখ্যা 11 টি

BSc. in CSE-17 Final Exam (Spring) Feb-21 পরীক্ষা(Examination), 20 21

বিষয় (Subj): Data and Network Security পত্র/কোর্স নং (Paper/Course No): CSE-429

পত্র/কোর্সের নাম (Paper/Course Name): CSE-17 কেন্দ্র (Center): MIST

রেজিঃ নম্বর (Regn No): 131401170018 শিক্ষাবর্ষ (Session): 2019-2020

রোল নম্বর (Roll No): 201714018 তারিখ (Date): 07-02-21

INSTRUCTIONS FOR EXAMINEE

1. Examinees are forbidden to write their names either on outer cover page or anywhere of the answer scripts. In case of violation, the answer script will not be evaluated.

2. Examinees must mention their roll and registration number along with session on the outer cover page of the answer scripts clearly. Otherwise, answer scripts may not be evaluated.

3. Students will write his examination roll number on the top left corner and section-A/B on the top right corner of each page. All pages must be numbered chronologically at the bottom center in x of y format. (for example: 1 of 21)

4. In no case, an examinee will be allowed to start the examination half an hour after the commencement of examination.

5. The Camera of the examinee MUST always be ON during the examination and answer script submission. If Camera is OFF then that online examination will be treated as CANCELLED.

6. The focus of the camera should be such that the invigilator(s) can see the script and examinee with his/her surroundings.

7. Students are to share their entire screen of desktop/laptop to the invigilator throughout the online examination. .

8. Browsing any files other than the given question paper (PDF) and/or online sites other than the respective allowed examination platform (e,g Zoom, Google classroom etc.) is strictly prohibited.

9. Online invigilators reserve the right to take remote access of the examinee's desktop/laptop and investigate as needed at any point during the examination or even after the examination

10. Students without laptop/desktop cannot appear exam online by using mobile phone. Students not possessing laptop/desktop, will have to appear examination Physically at MIST.

পরীক্ষক কর্তৃক পূরণীয়

প্রশ্ন নম্বর	প্রদত্ত নম্বর
১	
২	
৩	
৪	
৫	
৬	
৭	
৮	
৯	
১০	
১১	
১২	
১৩	
১৪	
মোট	

পরীক্ষকের স্বাক্ষর

নিরীক্ষকের স্বাক্ষর

Continued......

INSTRUCTIONS FOR EXAMINEE

11. Examinees must abide by the instructions of chief invigilator if there are no definite instructions on any subject/matter.

12. No examinee will be allowed to leave the examination session until an hour has elapsed from the commencement of examination.

13. Legal action will be taken against the examinees those are trying to adopt/adopting unfaimeans/exibiting unbecoming conduct in the examination hall and found guilty for any breach of discipline as per rule.

14. Invigilators will have complete authority of deducting marks from any student attempting unfair means.

15. All rough works should be done in the same paper used as answer scripts. Answer scripts should be submitted intact. Papers used for rough work should be pen through by the examinees and submitted along with the answer script.

16. The answer scripts submitted beyond specified time will be treated as CANCELLED.

17. The examinee will send his/her scanned examination script in PDF format to the following e-mail addresses:

    (a) e-mail address of subject invigilator/examiner.

    (b) Central Database Scheme (coursecode@mist.ac.bd)
    Example: EECE433@mist.ac.bd

18. The examinee has to preserve the original answer script of every examination and be ready to submit whenever asked for.

19. Answer script should be the A4 size papers with a cover page provided by Department. Examinee has to fill up his/her necessary details on the cover page. Section A and section B must be clearly marked on the cover page like. **Section A** or **Section B**

20. Examination duration for each subject will be two hours (section-A for one hour + section B for One hour). In between students will get 15 minutes time to submit the answer script of section A and 5 minutes time to issue the question for section B . After completion of 01 hour examination time for section B, students will get 15 minutes to submit the answer script of section B.

21. After completion of written examination (online/physical), viva will be conducted by the respective faculty of that subject.

Section-B

Ans. to the ques. no.-06(a)

RSA algorithm:

RSA algorithm uses expression with exponentials and is an encryption method that is very hard to attack fore large key values. RSA is also a public-key cryptography algorithm as it makes use of both public and a private keys.

To encrypt using RSA algorithm the following steps are needed to do:

1. Select two prime numbers p and q.
2. calculate, $n = pq$.
3. calculate, $\phi(n) = (p-1)(q-1)$
4. select, e such that, $\gcd(\phi(n), e) = 1$ and, $1 < e < \phi(n)$
5. calculate, d where, $d = e^{-1}(\mathrm{mod}(\phi(n)))$
6. Public key, $PU = \{e, n\}$
7. Private key, $PR = \{d, n\}$

P.T.O.

(8) To encrypt plaintext, m :

Ciphertext, c = $m^e \bmod n$.

(9) To decrypt :

~~c=~~ $M = c^d \bmod n$.

RSA is valid since for large values of p and q which are two prime numbers finding $n = pq$ or factoring $\phi(n)$ is very difficult and takes a very long time and without factoring $\phi(n)$ one cannot find the d which is the private key. So, RSA is (large p, q) a very good algorithm and is a valid algorithm as it also maintains diffusion and confusion.

Ans. to the ques. no.- 06(b)

Given,

$n = 55,$

$e = 3$

plaintext, $P = 12$ [captical, P]

So,

~~Φ(~~ let, p, q two prime numbers be 5 and 11 so that $n = pq = 55$.

So, $p = 5$

$q = 11$

$$\therefore \phi(n) = (5-1)(11-1)$$
$$= 40$$

and, we know, $d = e^{-1} \bmod (\phi(n))$

$$= 3^{-1} \bmod 40$$
$$= 27 \bmod 40$$
$$= 27$$

[Since, $3 \times 27 = 81$ and, $81 \equiv 1 \bmod 40$]

So, public key, $PU = \{e, n\} = \{3, 55\}$

private key, $PR = \{d, n\} = \{27, 55\}$

(i) Finding out ciphertext C of the Message P.

Here, P = 12.

So,

$$C = P^e \bmod n$$

$$= 12^3 \bmod 55 \qquad [e = 3, n = 55]$$

$$= 1728 \bmod 55$$

$$= 23$$

So, cipher value C = 23 (Ans)

(ii) We already calculated the d and know the private key = {d, n} = {27, 55}

So, if ciphertext, C = 23 and we will decrypt C to get the plaintext or message P.

$$P = C^d \bmod n$$

$$= 23^{27} \bmod 55 \qquad [\because d = 27 \text{ and } n = 55]$$

$$= ((23^3)^3)^3 \bmod 55 \qquad [((23)^3)^9 = (23)^{27}]$$

$$= ((23^3 \bmod 55)^3 \bmod 55)^3 \bmod 55 \qquad [\because \text{From Modular Algorithm}]$$

$$= (12^3 \bmod 55)^3 \bmod 55$$

$$= (23)^3 \bmod 55 = 12$$

So; Decrypted C using RSA decryption algorith and we get the message, P=12 (which is correct since, P=12 (given).]

(Ans)

Ans. to the ques. no.-06(c)

Different kinds of attacks ~~e~~ in RSA is discussed below:

① Brute-force Attack:

This attack involves trying (test and trial) all possible private keys to try to decrypt the message to get a meaning sentence. RSA can be attacked with Brute-force Attack. But if p and q are large then d is harder to find in Brute-force (take a long time.)

② Mathematical attack:

This attack involves factoring the product of the two primes to get $\phi(n)$. and eventually to get the value of d (private key).

③ Timing Attack:

It is possible to guess the decryption key from the time taken by a processor to decrypt the message using decryption algorithm. Timing attack involves monitioring the running time of the decryption algorithm.

④ Hardware fault-based attack:

This attack involves inducing hardware specifically processor (or motherboard) faults to generate some error in one bit during encryption and analyzing the error to guess the private key. But rare since, physicall access to Hardware is required for this Attack.

⑤ chosen ciphertext Attack:

This attack involves exploits properties of RSA Algorithm by chosen some specific ciphertext and get the output of decryption for getting the private key.

Ans. to the ques. no.- 05(a)

Public-key cryptography is very effective since it uses the concepts of public key so it is secure for key exchange in a public channel. But Public-key cryptography is not efficient. Since, Public-key Cryptography needs two keys: Public key and Private key. The key sizes must be large or else it is vulnerable to Brute-force attack. But the proposed key sizes are infeasible to use in general real life cases. As large key sizes largely impacts on the algorithm and performance speed. But for secure key exchange, authentication Public-key cryptography can be used in ~~real~~ real life.

symmetric key cryptography is used where

P.T.O.

sender and receiver shares a secret and uses the same key to encrypt and decrypt. symmetric key cryptography requires the one secret key to be shared to the receiver from sender. But sharing secret key in a public channel is not secure. But symmetric key-cryptography is very good and feasible in real life situations and is very efficient and has very good performance speed for large key values.

So, while public key cryptography is effective it is not efficient and while symmetric key cryptography is efficient it is not ~~b~~ very effective (key share). So, they are complementary to each other.

In real life, both of them used at the same time for acheiving the advantages of both at the same time.

Ans. to the ques. no.- 05(b)

I considere Diffie-Hellman algorithm just for a key exchange algorithm.. The algorithm is following bellow steps!

① Source A picks random number X_A, and ~~Source~~ Destination B pick picks a random number X_B.

② A selects q a large prime number and α = primitive root of q.

③ A calculates:

$$Y_A = \alpha^{X_A} \bmod q$$ and ~~sends~~

sends α, q, Y_A

④ B calculates:

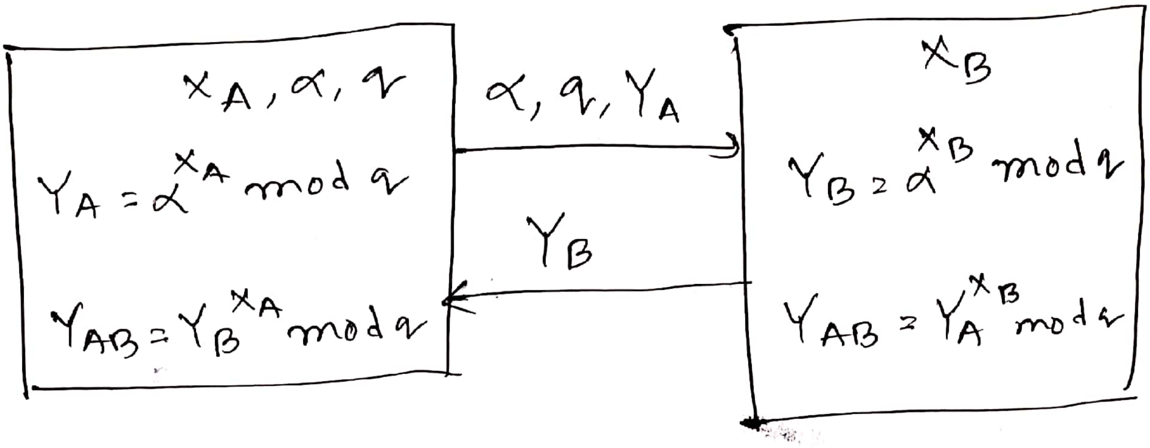
$$Y_B = \alpha^{X_B} \bmod q$$

and sends Y_B

⑤ A gets : $Y_{AB} = Y_B^{X_A} \bmod q$

⑥ B gets $Y_{AB} = Y_A^{X_B} \bmod q$.

P.T.O.


X_A, α, q
$Y_A = \alpha^{X_A} \bmod q$
$Y_{AB} = Y_B^{X_A} \bmod q$
α, q, Y_A
Y_B
X_B
$Y_B = \alpha^{X_B} \bmod q$
$Y_{AB} = Y_A^{X_B} \bmod q$

Ultimately, $Y_{AB} = \alpha^{X_A X_B} \bmod q$.

Fig: Diffie-Hellmann Key Exchance

Since, it doest not involve public-key concepts I will consider Diffie-Hellmann algorithm as just a key exchange algorithm. as it shares the X_A key to X_B ~~seque~~ securely and is authenticated. So, Diffie-Hellmann is a good key exchange algorithm in my opinion.

Ans. to the ques. no.. 05(c)

A big drawback of Diffie-Hellmann algorithm is the man-in-the-middle attack.

Man-in-the middle attack happens when some in the middle intercepts messages from source and replay to the destination.

we can use RSA algorithm and other encryption algorithm for the authentication of source and also destination. Having authentication in place, if the man-in-the-middle changes or modifies the message other ~~we~~ can get that from the authentication part that someone changes. So, RSA algo to authentication is a way to avert that.

—x—