Enrollment No./Seat No.:

# GUJARAT TECHNOLOGICAL UNIVERSITY

**DIPLOMA IN ENGINEERING - SEMESTER - III EXAMINATION - WINTER 2025**

**Subject Code: DI03016021** **Date: 06-12-2025**

**Subject Name: Cryptography and Web Security**

**Time: 10:30 AM TO 01:00 PM** **Total Marks: 70**

**Instructions:**

1. **Attempt all questions.**
2. **Make Suitable assumptions wherever necessary.**
3. **Figures to the right indicate full marks.**
4. **Use of simple calculators and non-programmable scientific calculators are permitted.**
5. **English version is authentic.**

**Marks**

**Q.1** **(a)** With the reference to computer security, explain confidentiality, integrity and availability. **03**

**(અ)** કોમ્પ્યુટર સિક્યોરીટીના સંદર્ભ માં કોન્ફિડેન્શ્યાલીટી, ઇન્ટીગ્રીટી અને અવેલેબિલિટી સમજાવો. ૦૩

**(b)** Encrypt the given plain-text using Additive cipher algorithm. Show the modular arithmetic calculation for encryption. **04**

Plain-text: "transform" Key: 9

**(બ)** આપેલ પ્લેન-ટેક્સ્ટ ને એડીટીવ સાયફર અલ્ગોરિધમનો ઉપયોગ કરીને એનક્રીપ્ટ કરો. એનક્રીપ્શન માટે મોડ્યુલર ગણિતની ગણતરી દર્શાવો. ૦૪

પ્લેન-ટેક્સ્ટ: "transform" કી: 9

**(c)** Write the Euclidean algorithm. Find the GCD(Greatest Common Divisor) of 1064 and 940 using the algorithm. Show each step of the algorithm calculation in tabular format as given below. **07**

| q | r1 | r2 | r |
|---|---|---|---|
| | | | |

**(ક)** યુક્લિડિયન અલ્ગોરિધમ લખો. આ અલ્ગોરિધમનો ઉપયોગ કરીને 1064 અને 940 નો ગુ.સા.અ. (ગુરુત્તમ સામાન્ય અવયવ) શોધો. અલ્ગોરિધમની ગણતરીના દરેક પગલા નીચે આપેલ કોષ્ટક માં દર્શાવો. ૦૭

| q | r1 | r2 | r |
|---|---|---|---|
| | | | |

**OR**

**(c)** Write extended Euclidean algorithm. Find the multiplicative inverse of 19 in $Z_{35}$ using the algorithm. Show the each step of algorithm calculation in tabular format as given below: **07**

| q | r1 | r2 | r | s1 | s2 | s |
|---|---|---|---|---|---|---|
| | | | | | | |

**(ક)** એક્સટેન્ડેડ યુક્લિડિયન અલ્ગોરિધમ લખો. આ અલ્ગોરિધમનો ઉપયોગ કરીને $Z_{35}$ માં 19 નો મલ્ટીપ્લિકેટીવ ઇનવર્સ શોધો. અલ્ગોરિધમની ગણતરીના દરેક પગલા નીચે આપેલ કોષ્ટક માં દર્શાવો. **૦૭**

| q | r1 | r2 | r | s1 | s2 | s |
|---|---|---|---|---|---|---|
| | | | | | | |

**Q.2** **(a)** Explain divisibility and division algorithm. **03**

**(અ)** ડિવીઝીબીલીટી અને ડિવિઝન અલ્ગોરિધમ સમજાવો. **૦૩**

**(b)** Draw the model for network security and explain. **04**

**(બ)** નેટવર્ક સિક્યોરીટીનું માળખું દોરો અને સમજાવો. **૦૪**

**(c)** Explain six security services in detail. **07**

**(ક)** છ સિક્યોરીટી સેવાઓને વિગતવાર સમજાવો. **૦૭**

**OR**

**(a)** If a = 12, b = 11 and n = 7 then prove that (a × b) mod n = [(a mod n) × (b mod n)] mod n. **03**

**(અ)** જો a = 12, b = 11 અને n = 7 તો સાબિત કરો કે (a × b) mod n = [(a mod n) × (b mod n)] mod n. **૦૩**

**(b)** With reference to modular arithmetic, explain the sets $Z_n$ and $Z_n$*. Provide the members of the set $Z_7$ and $Z_7$*. **04**

**(બ)** મોડ્યુલર ગણિતના સંદર્ભમાં, ગણ $Z_n$ અને $Z_n$* સમજાવો. $Z_7$ અને $Z_7$* ગણના સભ્યો જણાવો. **૦૪**

**(c)** Explain two passive and four active attacks of network security. **07**

**(ક)** નેટવર્ક સિક્યોરીટીના બે પેસિવ(પરોક્ષ) અને ચાર એક્ટિવ(પ્રત્યક્ષ) હુમલાઓ સમજાવો. **૦૭**

**Q.3** **(a)** Explain stream cipher and block cipher with example. **03**

**(અ)** સ્ટ્રીમ સાયફર અને બ્લોક સાયફર ઉદાહરણ સાથે સમજાવો. **૦૩**

**(b)** Explain working of Autokey cipher with example. **04**

**(બ)** ઓટોકી સાયફરની કાર્ય પધ્ધતિ ઉદાહરણ સાથે સમજાવો. **૦૪**

**(c)** Convert the given plain-text: "decisions" into cipher-text using Hill cipher. Show all the steps for calculation. **07**

Plain-text: $\begin{bmatrix} d & e & c \\ i & s & i \\ o & n & s \end{bmatrix}$ key: $\begin{bmatrix} 5 & 7 & 10 \\ 3 & 1 & 7 \\ 0 & 5 & 2 \end{bmatrix}$

**(ક)** આપેલ પ્લેન-ટેક્સ્ટ: "decisions" ને હિલ સાયફરનો ઉપયોગ કરીને સાયફર-ટેક્સ્ટમાં ફેરવો. ગણતરીના બધા જ પગલાં બતાવો. **૦૭**

પ્લેન-ટેક્સ્ટ: $\begin{bmatrix} d & e & c \\ i & s & i \\ o & n & s \end{bmatrix}$ કી: $\begin{bmatrix} 5 & 7 & 10 \\ 3 & 1 & 7 \\ 0 & 5 & 2 \end{bmatrix}$

**OR**

| | | | |
|---|---|---|---|
| | **(a)** | Explain keyed transposition cipher with example. | **03** |
| | **(અ)** | કીવાળું ટ્રાન્સપોઝિશન સાયફર ઉદાહરણ સાથે સમજાવો. | ૦૩ |
| | **(b)** | Encrypt the given plaint-text: "battery" using Playfair cipher. The key : FORUM | **04** |
| | **(બ)** | આપેલ પ્લેન-ટેક્સ્ટ: "battery" ને પ્લેફેર સાયફરનો ઉપયોગ કરી એન્ક્રીપ્ટ કરો. તે માટેની કી: FORUM | ૦૪ |
| | **(c)** | Explain key-generation of RSA with example. Show encryption and decryption using RSA algorithm with example. | **07** |
| | **(ક)** | RSAનું કી-જનરેશન ઉદાહરણ સાથે સમજાવો. RSA અલ્ગોરિધમનો ઉપયોગ કરીને એન્ક્રીપ્શન અને ડીક્રીપ્શન પ્રક્રિયા ઉદાહરણ સાથે દર્શાવો. | ૦૭ |
| **Q.4** | **(a)** | Discuss the web security threats on integrity and confidentiality. | **03** |
| | **(અ)** | ઇન્ટીગ્રીટી અને કોન્ફિડેન્શ્યાલીટી પર વેબ સિક્યોરીટીની ખતરાઓ / ધમકીઓની ચર્ચા કરો. | ૦૩ |
| | **(b)** | Draw and discuss SSL protocol stack in short. | **04** |
| | **(બ)** | SSL પ્રોટોકોલ સ્ટેક દોરો અને ટૂંકમાં સમજાવો. | ૦૪ |
| | **(c)** | For secure electronic transaction, explain role of its participants. Enlist sequence of events occur during transaction. | **07** |
| | **(ક)** | સિક્યોર ઇલેક્ટ્રોનિક ટ્રાન્ઝેક્શન માટેના સહભાગીઓની ભૂમિકા સમજાવો. ટ્રાન્ઝેક્શન દરમ્યાન થતી ઘટનાઓની ક્રમશ: યાદી બનાવો. | ૦૭ |
| | | **OR** | |
| | **(a)** | To provide web security, discuss the approaches at network, transport and application level. | **03** |
| | **(અ)** | વેબ સિક્યોરીટી આપવા માટે, નેટવર્ક, ટ્રાન્સપોર્ટ અને એપ્લિકેશન લેવલ પરના અભિગમોની ચર્ચા કરો. | ૦૩ |
| | **(b)** | Give the full form of TLS and HTTPS. Explain HTTPS connection initiation. | **04** |
| | **(બ)** | TLS અને HTTPS ના પૂરા નામ આપો. HTTPS કનેક્શન ઇનિશ્યેશન સમજાવો. | ૦૪ |
| | **(c)** | Compare SSL (Secure Socket Layer) with SET (Secure Electronic Transaction). | **07** |
| | **(ક)** | SSL(સિકયોર સોકેટ લેયર) અને SET (સિક્યોર ઇલેક્ટ્રોનિક ટ્રાન્ઝેક્શન) ની સરખામણી કરો. | ૦૭ |
| **Q.5** | **(a)** | If the key is 11 and its multiplicative inverse key = 19 then, decrypt the cipher-text: "dagcqo" which is encrypted using multiplicative cipher algorithm. | **03** |
| | **(અ)** | જો કી 11 હોય અને તેની મલ્ટીપ્લીકેટીવ ઇનવર્સ (વ્યસ્ત) કી = 19 હોય તો, સાયફર-ટેક્સ્ટ: "dagcqo" ને ડીક્રીપ્ટ કરો કે જેને મલ્ટીપ્લીકેટીવ સાયફર અલ્ગોરિધમથી એન્ક્રીપ્ટ કરેલ છે. | ૦૩ |
| | **(b)** | Explain the need of firewall in the network security. | **04** |
| | **(બ)** | નેટવર્ક સિક્યોરીટીમાં ફાયરવોલ ની જરૂરિયાત સમજાવો. | ૦૪ |
| | **(c)** | Define intrusion, intrusion detection and intrusion detection system. Explain misuse detection and anomaly detection approaches of intrusion detection. | **07** |
| | **(ક)** | ઇન્ટ્રુઝન (ઘુસણખોરી), ઇન્ટ્રુઝન ડિટેક્શન અને ઇન્ટ્રુઝન ડિટેક્શન પધ્ધતિ વ્યાખ્યાયિત કરો. ઇન્ટ્રુઝન ડિટેક્શનના મિસયુઝ ડિટેક્શન અને એનોમલી ડિટેક્શન અભિગમો સમજાવો. | ૦૭ |

**OR**

| | | |
|---|---|---|
| **(a)** | Explain the categories of the intruders in the system security. | **03** |
| **(અ)** | સિસ્ટમ સિક્યોરીટીમાં ઘૂસણખોરોની શ્રેણીઓ સમજાવો. | ૦૩ |
| **(b)** | Explain the working of one-time pad algorithm with example. | **04** |
| **(બ)** | વન-ટાઈમ પેડની કાર્ય પધ્ધતિ ઉદાહરણ સાથે સમજાવો. | ૦૪ |
| **(c)** | Explain packet filtering firewall, application and circuit-level gateway. | **07** |
| **(ક)** | પેકેટ ફિલ્ટરીંગ ફાયરવોલ, એપ્લિકેશન અને સર્કીટ-લેવલ ગેટવે સમજાવો. | ૦૭ |

***