| Reg. No. | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|

**MANIPAL INSTITUTE OF TECHNOLOGY**
MANIPAL
*(A constituent unit of MAHE, Manipal)*

## DEPARTMENT OF MECHATRONICS

## VII SEMESTER B.TECH. (MECHATRONICS)

## END SEMESTER EXAMINATIONS (PART-A), December 2021

## SUBJECT: PRINCIPLES OF CRYPTOGRAPHY [MTE 4058]

**(Date: December 27, 2021)**

**Time: 45 + 5 Minutes** **MAX. MARKS: 30**

**Instructions to Candidates:**

- Answer **ALL** the questions.

| Q. No | | M | CO | PO | LO | BL |
|---|---|---|---|---|---|---|
| | **MCQ Type Questions (1 × 30 = 30)** | | | | | |
| **1.** | In S-DES algorithm, the 4-bit input to E/P (Expansion/Permutation) block is 0110. The output generated is ______.<br>a. 11001100<br>b. 00111100<br>c. 11000011<br>d. 00110011 | **1** | **1** | **1** | **1** | **3** |
| **2.** | The plaintext is "WEWEREOLD", the encryption key is "DECEPTIVE", the algorithm is "Vignere Cipher". The ciphertext produced is ______.<br>a. "ZIYIGXWGH"<br>b. "HGWXGIYIZ"<br>c. "AJZJHYXHI"<br>d. "IHXYHJZJA" | **1** | **1** | **2** | **2** | **3** |
| **3.** | The plaintext is "IAMTHEBEST", the encryption key is 2 rails, the algorithm is "The Rail-Fence Cipher". The ciphertext produced is ______.<br>a. "ATEETIMHBS"<br>b. "IMHBSATEET"<br>c. "IMATHBEEST"<br>d. "IAMTHEBEST" | **1** | **1** | **2** | **2** | **3** |
| **4.** | The plaintext is "IAMTHEBEST", the encryption key is 3 rails, the algorithm is "The Rail-Fence Cipher". The ciphertext produced is ______.<br>a. "ATEETIHSMB"<br>b. "MBATEETIHS"<br>c. "IHSATEETMB"<br>d. "IHSMBATEET" | **1** | **1** | **2** | **2** | **3** |
| **5.** | The plaintext is "MITMANIPAL", the encryption key is 'A', and the algorithm is "Caesar Cipher". The ciphertext developed is _____.<br>a. "NJUNBOJQBM"<br>b. "LHSLZMHOZK"<br>c. "MITMANIPAL"<br>d. "LAPINAMTIM" | **1** | **1** | **2** | **2** | **3** |
| **6.** | The plaintext is "ATTACKNOW", the encryption key is (3 1 2), and the algorithm is "Columnar Transposition Technique". The ciphertext | **1** | **1** | **2** | **2** | **3** |

<table>
<tr><td></td><td>produced is _____.<br>a. “TCOTKWAAN”<br>b. “TKWTCOAAN”<br>c. “AANTCOTKW”<br>d. “AANTKWTCO”</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td><b>7.</b></td><td>The plaintext is “MECHATRONICS”, the encryption key is “DEPARTMENT”, and the algorithm is “Playfair Cipher”. The ciphertext produced is _______.<br>a. “UBHBUEBDKNMG”<br>b. “BUBHEUDBNKGM”<br>c. “GMNKDBEUBHBU”<br>d. “MGKNBDUEHBUB”</td><td><b>1</b></td><td><b>1</b></td><td><b>2</b></td><td><b>2</b></td><td><b>3</b></td></tr>
<tr><td><b>8.</b></td><td>In DES algorithm, the input to S-Box 1 is 100011. The output generated is _______.
<table>
<tr><th></th><th>0</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>10</th><th>11</th><th>12</th><th>13</th><th>14</th><th>15</th></tr>
<tr><td>0</td><td>14</td><td>04</td><td>13</td><td>01</td><td>02</td><td>15</td><td>11</td><td>08</td><td>03</td><td>10</td><td>06</td><td>12</td><td>05</td><td>09</td><td>00</td><td>07</td></tr>
<tr><td>1</td><td>00</td><td>15</td><td>07</td><td>04</td><td>14</td><td>02</td><td>13</td><td>10</td><td>03</td><td>06</td><td>12</td><td>11</td><td>09</td><td>05</td><td>03</td><td>08</td></tr>
<tr><td>2</td><td>04</td><td>01</td><td>14</td><td>08</td><td>13</td><td>06</td><td>02</td><td>11</td><td>15</td><td>12</td><td>09</td><td>07</td><td>03</td><td>10</td><td>05</td><td>00</td></tr>
<tr><td>3</td><td>15</td><td>12</td><td>08</td><td>02</td><td>04</td><td>09</td><td>01</td><td>07</td><td>05</td><td>11</td><td>03</td><td>14</td><td>10</td><td>00</td><td>06</td><td>13</td></tr>
</table>
a. 08<br>b. 12<br>c. 05<br>d. 02</td><td><b>1</b></td><td><b>1</b></td><td><b>1</b></td><td><b>1</b></td><td><b>3</b></td></tr>
<tr><td><b>9.</b></td><td>The plaintext is “INDIA”, the encryption key is ‘PIANO’, and the algorithm is “Book Cipher or Running Key Cipher”. The ciphertext developed is _____.<br>a. “OFDFH”<br>b. “OVDVX”<br>c. “HFDFO”<br>d. “XVDVO”</td><td><b>1</b></td><td><b>1</b></td><td><b>2</b></td><td><b>2</b></td><td><b>3</b></td></tr>
<tr><td><b>10.</b></td><td>Compute $\phi(35)$ using Euler’s Totient function.<br>a. 10<br>b. 12<br>c. 24<br>d. 34</td><td><b>1</b></td><td><b>2</b></td><td><b>1</b></td><td><b>1</b></td><td><b>3</b></td></tr>
<tr><td><b>11.</b></td><td>Compute $\phi(125)$ using Euler’s Totient function.<br>a. 124<br>b. 110<br>c. 100<br>d. 75</td><td><b>1</b></td><td><b>2</b></td><td><b>1</b></td><td><b>1</b></td><td><b>3</b></td></tr>
<tr><td><b>12.</b></td><td>In AES algorithm, the key size is 256-bits and the plaintext block size is 128-bits. The number of round encryption operation is _____.<br>a. 10<br>b. 12<br>c. 14<br>d. 16</td><td><b>1</b></td><td><b>2</b></td><td><b>2</b></td><td><b>2</b></td><td><b>3</b></td></tr>
<tr><td><b>13.</b></td><td>In AES algorithm, the key size is 128-bits and the plaintext block size is 128-bits. The number of round encryption operation is _____.<br>a. 10<br>b. 12<br>c. 14<br>d. 16</td><td><b>1</b></td><td><b>2</b></td><td><b>2</b></td><td><b>2</b></td><td><b>3</b></td></tr>
<tr><td><b>14.</b></td><td>The Fermat’s theorem $a^{p-1} \equiv 1 \pmod{p}$ is used if<br>a. <i>‘p’</i> is prime and <i>‘a’</i> is a positive integer<br>b. <i>‘p’</i> is prime and <i>‘a’</i> is a positive integer not divisible by <i>‘p’</i><br>c. <i>‘p’</i> is prime, <i>‘a’</i> is a positive integer not divisible by <i>‘p’</i>, and <i>‘a’</i> be relative prime to <i>‘p’</i>.</td><td><b>1</b></td><td><b>2</b></td><td><b>1</b></td><td><b>1</b></td><td><b>1</b></td></tr>
</table>

| | | | | | | |
|---|---|---|---|---|---|---|
| | d. None of these | | | | | |
| **15.** | The Fermat's theorem $a^p \equiv a\ (mod\ p)$ is used if<br>a. *'p'* is prime and *'a'* is a positive integer<br>b. *'p'* is prime and *'a'* is a positive integer not divisible by *'p'*<br>c. *'p'* is prime, *'a'* is a positive integer not divisible by *'p'*, and *'a'* be relative prime to *'p'*.<br>d. None of these | **1** | **2** | **1** | **1** | **1** |
| **16.** | If $n = p^e$, determine $\phi(n)$.<br>a. $\phi(n) = p^{e-1} - p^{e-2}$<br>b. $\phi(n) = p^e - p^{e-1}$<br>c. $\phi(n) = p^{e+1} - p^e$<br>d. $\phi(n) = p^{e+2} - p^{e+1}$ | **1** | **2** | **2** | **2** | **4** |
| **17.** | In stream cipher, _____ stream is used for encryption and decryption operation.<br>a. Random number<br>b. Pseudorandom number<br>c. Fixed sequence number<br>d. None of the above | **1** | **2** | **1** | **1** | **1** |
| **18.** | Generate the residue class [1] of $(mod\ 3)$, where "*mod*" represents the modulus operation.<br>a. {…, -9, -6, -3, 1, 3, 6, 9, …}<br>b. {…, -8, -5, -2, 1, 4, 7, 10, …}<br>c. {…, -7, -4, -1, 1, 5, 8, 11, …}<br>d. {…, -10, -7, -4, 1, 2, 5, 8, …} | **1** | **2** | **1** | **1** | **3** |
| **19.** | Solve $-29\ mod\ 7$, where "*mod*" denotes the modulus operation.<br>a. – 1<br>b. 1<br>c. 6<br>d. – 6 | **1** | **2** | **1** | **1** | **3** |
| **20.** | Compute the GCD of 316258250 and 211943424 using Euclidean algorithm.<br>a. 1002<br>b. 1014<br>c. 1056<br>d. 1078 | **1** | **2** | **1** | **1** | **3** |
| **21.** | The plaintext, $M = 6$, the two prime numbers, $p = 7$ and $q = 17$, the public key or encryption key, $e = 5$, and the algorithm is "RSA". The ciphertext produced is ______.<br>a. 26<br>b. 27<br>c. 28<br>d. 29 | **1** | **3** | **2** | **2** | **3** |
| **22.** | ______ is the prime function of Diffie-Hellman algorithm.<br>a. Encryption-decryption operation<br>b. Hash value generation operation<br>c. Key exchange operation<br>d. None of these | **1** | **3** | **1** | **1** | **1** |
| **23.** | The primitive roots of 7 are ______.<br>a. Both 2 and 3<br>b. Both 4 and 5<br>c. Both 2 and 5<br>d. Both 3 and 5 | **1** | **3** | **1** | **1** | **3** |
| **24.** | The private key $X_A$ of user $A$ is 3, the public key $Y_B$ of user $B$ is 2, the prime factor or global element $q$ is 7, and the algorithm is "Diffie-Hellman". The secret key generated by user $A$ is ______.<br>a. 1 | **1** | **3** | **1** | **1** | **3** |

| | | | | | | |
|---|---|---|---|---|---|---|
| | b. 2<br>c. 3<br>d. 4 | | | | | |
| **25.** | The private key $X_B$ of user $B$ is 4, the public key $Y_A$ of user $A$ is 6, the prime factor or global element $q$ is 7, and the algorithm is "Diffie-Hellman". The secret key generated by user $B$ is ______.<br>a. 1<br>b. 2<br>c. 3<br>d. 4 | **1** | **3** | **1** | **1** | **3** |
| **26.** | The prime number $p$ is 11, the decryption key or private key $D$ is 3, the second part of encryption key or public key $E_1$ is 2, and the algorithm is "ElGamal Cryptosystem". The third part of encryption key or public key $E_2$ generated is ______.<br>a. 4<br>b. 6<br>c. 8<br>d. 10 | **1** | **3** | **1** | **1** | **3** |
| **27.** | The random integer $R$ is 4, the second part of encryption key or public key $E_1$ is 2, and the algorithm is "ElGamal Cryptosystem". The first part of ciphertext $C_1$ produced is ______.<br>a. 4<br>b. 5<br>c. 6<br>d. 7 | **1** | **3** | **2** | **2** | **3** |
| **28.** | The message authentication code (MAC) is developed to generate _______ hash function.<br>a. Fixed keyed<br>b. Variable keyed<br>c. Fixed non-keyed<br>d. Variable non-keyed | **1** | **4** | **1** | **1** | **1** |
| **29.** | In SHA-1 hash algorithm, the message digest generated is _____.<br>a. 160 bits<br>b. 180 bits<br>c. 256 bits<br>d. 512 bits | **1** | **4** | **1** | **1** | **1** |
| **30.** | In SHA-512 hash algorithm, the message digest generated is _____.<br>a. 160 bits<br>b. 180 bits<br>c. 256 bits<br>d. 512 bits | **1** | **4** | **1** | **1** | **1** |