Register Number | | | | | | | | |

Sri Sivasubramaniya Nadar College of Engineering, Kalavakkam – 603 110

(An Autonomous Institution, Affiliated to Anna University, Chennai)

Department of Computer Science and Engineering

Continuous Assessment Test – I Answer key

Question Paper

Degree & Branch	B.E CSE				**Semester**	V
Subject Code & Name	UCS1505 & INTRODUCTION TO CRYPTOGRAPHIC TECHNIQUES				**Regulation: 2018**	
Academic Year	2022-23 ODD	**Batch**	2020-24	**Date**	**21.09.2022**	**FN**
Time: 8.15 – 9.45 AM (90 Minutes)	**Answer All Questions**				**Maximum: 50 Marks**	

Part – A (6×2 = 12Marks)

K2	1. Outline the formal definition of the Gen, Enc, and Dec algorithms for the mono-alphabetic substitution cipher. **Answer** $\mathcal{M}$ is then any finite sequence of integers from this set. Encryption of the message $m = m_1 \cdots m_\ell$ (where $m_i \in \{0, \ldots, 25\}$) using key k is given by $$\mathsf{Enc}_k(m_1 \cdots m_\ell) = c_1 \cdots c_\ell, \quad \text{where } c_i = [(m_i + k) \bmod 26].$$ (The notation $[a \bmod N]$ denotes the remainder of a upon division by N, with $0 \le [a \bmod N] < N$. We refer to the process mapping a to $[a \bmod N]$ as *reduction modulo* N; see also Chapter 9.) Decryption of a ciphertext $c = c_1 \cdots c_\ell$ using key k is given by $$\mathsf{Dec}_k(c_1 \cdots c_\ell) = m_1 \cdots m_\ell, \quad \text{where } m_i = [(c_i - k) \bmod 26].$$	CO1	1.4.1
K2	2. Show how many keys are required for two people to communicate via symmetric and asymmetric ciphers? **Answer** Symmetric: One asymmetric ciphers : Two	CO1	1.3.1
K3	3. Apply the Vigenère cipher and decrypt the ciphertext VEQPJIREDOZXOE with the key café. **Answer** Plaintext: `tellhimaboutme` Key (repeated): `cafecafecafeca` Ciphertext: `VEQPJIREDOZXOE`	CO1	1.4.1
K2	4. Outline Kerchoff's principle and justify it. **Answer** The cipher method must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience.	CO1	1.3.1 1.4.1
K3	5. Compare and contrast the encryption, MAC and Hash functions **Answer** MAC: Accepts arbitrary length message Hash: Accepts arbitrary length message MAC: Generates fixed length output as MAC/tag Hash: Generates fixed length output as Hash code/ message digest MAC: Uses Key Hash: Does not use key MAC: Not reversible Hash: Not reversible	CO2	1.3.1 2.4.3

K2	6. Summarize the properties of hash function. **Answer** 1. can be applied to any size message `M` 2. produces a fixed-length output `h` 3. is easy to compute `h=H(M)` for any message `M` 4. given `h` is infeasible to find `x` s.t. `H(x)=h` - one-way property 5. given `x` is infeasible to find `y` s.t. `H(y)=H(x)` - weak collision resistance 6. is infeasible to find any `x,y` s.t. `H(y)=H(x)` - strong collision resistance	CO2	1.4.1

Part – B (3×6 = 18 Marks)

K3	7. Caesar wants to arrange a secret meeting with Marc Antony, either at the Tiber (the river) or at the Coliseum (the arena). He sends the shift cipher text EVIRE. However, Antony does not know the key, so he tries all possibilities. Apply the appropriate decryption algorithm and deduce where he will meet Caesar? **Answer** Using shift cipher with shift 3 and 13 Among the shifts of EVIRE, there are two words: arena and river. Therefore, Anthony cannot determine where to meet Caesar	CO1	1.4.1 13.3.1
K3	8. Assume an attacker knows that a user's password is either *abcd* or *bedg*. Say the user encrypts his password using the shift cipher, and the attacker sees the resulting ciphertext. Apply the appropriate decryption algorithm and show how the attacker can determine the user's password or explain why this is not possible. **Answer** The alphabet {A,B,...,Z} with the set $\Sigma = \{0,1,...25\}$ and all additions are implicitly taken mod 26. Then the possible passwords are p0 = abcd = (0,1,2,3) and p1 = bedg = (1,4,3,6). Note that all possible encryptions of p0 are $C0 = \{(k,k + 1,k + 2, k +3) \mid k \in \Sigma\}$ and the ones of p1 are $C1 = \{(k +1,k +4,k +3,k +6) \mid k \in \Sigma\}$. These two sets are disjoint and so checking in which set the ciphertext lies allows to deduce the password.	CO1	1.4.1 13.3.1
K2	9. Outline the formal definition for the construction of CBC MAC with proper illustration. **Answer** Let F be a pseudorandom function, and fix a length function $\ell(n) > 0$. The basic CBC-MAC construction is as follows: • Mac: on input a key $k \in \{0,1\}^n$ and a message m of length $\ell(n) \cdot n$, do the following (set $\ell = \ell(n)$ in what follows): 1. Parse m as $m = m_1, \ldots, m_\ell$ where each m_i is of length n. 2. Set $t_0 := 0^n$. Then, for $i = 1$ to ℓ, set $t_i := F_k(t_{i-1} \oplus m_i)$. Output t_ℓ as the tag. • Vrfy: on input a key $k \in \{0,1\}^n$, a message m, and a tag t, do: If m is not of length $\ell(n) \cdot n$ then output 0. Otherwise, output 1 if and only if $t \stackrel{?}{=} \mathsf{Mac}_k(m)$.	CO2	1.4.1 13.3.1

Part – C (2×10 = 20 Marks)

K3	10. Let (E, D) be a semantically secure cipher with key space $K = \{0,1\}^l$. A bank wishes to split a decryption key $k \in \{0,1\}^l$ into two pieces p_1 and p_2 so that both are needed for decryption. The piece p_1 can be given to one executive and $p_2$to another so that both must contribute their pieces for decryption to proceed. The bank generates random k_1 in $\{0,1\}^l$ and sets $k_1' \leftarrow k \oplus k_1$. Note that $k_1 \oplus k_1' \rightarrow k$. The bank can give k_1 to one executive and k_1' to another. Both must be present for decryption to proceed since, by itself, each piece contains no information about the secret key k (note that each piece is a one-time pad encryption of k). Now, suppose the bank wants to split k into three pieces p_1, p_2, p_3 so that any two of the pieces enable decryption using k. This ensures that even if one executive is out sick, decryption can still succeed. To do so the bank generates two random pairs (k_1, k_1') and (k_2, k_2') as in the previous paragraph so that $k_1 \oplus k_1' = k_2 \oplus k_2' = k$. Solve the given problem and show how the bank assign pieces, so that any two pieces enable decryption using k, but no single piece can decrypt? Check whether this combination of the keys $p_1 = (k_1, k_2)$, $p_2 = (k_1')$, $p_3 = (k_2')$works, if not provide the correct combination. **Answer** The bank generates random k1 in {0,1}ℓ and sets k1'←k⊕k1. Note that k1⊕k1'=k. The bank can give k1 to one executive and k1' to another. Both must be present for decryption to proceed since, by itself, each piece contains no information about the secret key k (note that each piece is a one-time pad encryption of k). Now, suppose the bank wants to split k into three pieces p1,p2,p3 so that any two of the pieces enable decryption using k. This ensures that even if one executive is out sick, decryption can still succeed. To do so the bank generates two random pairs (k1,k1') and (k2,k2') as in the previous paragraph so that k1⊕k1'=k2⊕k2'=k. How should the bank assign pieces so that any two pieces enable decryption using k, but no single piece can decrypt? • ☐ p1=(k1,k2), p2=(k1,k2), p3=(k2') • ☐ p1=(k1,k2), p2=(k1',k2'), p3=(k2') • ☑ p1=(k1,k2), p2=(k1',k2), p3=(k2') • ☐ p1=(k1,k2), p2=(k2,k2'), p3=(k2') • ☐ p1=(k1,k2), p2=(k1'), p3=(k2') Explanation Combinations 1,2,5 cannot decrypt when any 2 people come together. Combination 4 can decrypt when only p2 is present. Thus, combination 3 is the only solution	CO1	1.4.1 13.3.1
OR			

K3

11. Apply the concept of perfect secrecy and prove that the cryptosystem built is perfectly secure?

$$P(X=a)=\frac{1}{2}, P(X=b)=\frac{1}{3}, P(X=c)=\frac{1}{6}$$

$$P(K=k_1)=P(K=k_2)=P(K=k_3)=\frac{1}{3}$$

Plaint text $P=\{a,b,c\}$, Cipher text $C=\{1,2,3,4\}$

Encryption Matrix

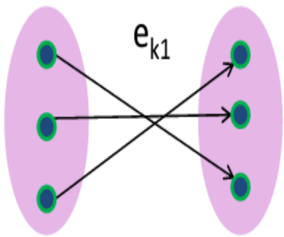
	a	b	c
k1	1	2	3
k2	2	3	4
k3	3	4	1

Answer

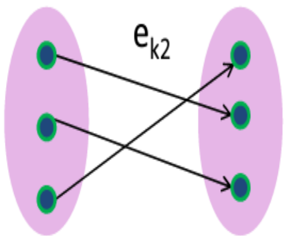
Key Distribution

- Alice & Bob agree upon a key k chosen from a key set $\mathbb{K}$
- Let ***K*** be a random variable denoting this choice

keyspace
Pr[**K**=k_1] = ¾
Pr[**K**=k_2] = ¼



There are two keys in the keyset thus there are two possible encryption mappings



CO1

1.4.1
13.3.1

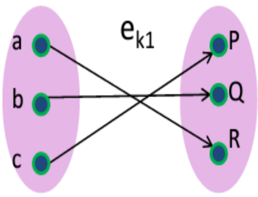
- Let **Y** be a discrete random variable over the set $\mathcal{C}$
- The probability of obtaining a particular ciphertext y depends on the plaintext and key probabilities

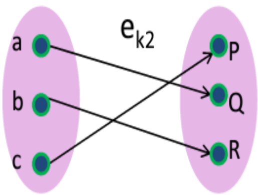
$$\Pr[Y=y]=\sum_k \Pr(k)\Pr(d_k(y))$$

Pr[Y = P] = $\Pr(k_1)$ * Pr(c) + $\Pr(k_2)$ * Pr(c)
= (3/4 * 1/6) + (1/4 * 1/6) = **1/6**

Pr[Y = Q] = $\Pr(k_1)$ * Pr(b) + $\Pr(k_2)$ * Pr(a)
= (3/4 * 1/3) + (1/4 * 1/2) = **3/8**

Pr[Y = R] = $\Pr(k_1)$ * Pr(a) + $\Pr(k_2)$ * Pr(b)
= (3/4 * 1/2) + (1/4 * 1/3) = **11/24**





plaintext
Pr[**X**=a] = 1/2
Pr[**X**=b] = 1/3
Pr[**X**=c] = 1/6

keyspace
Pr[**K**=k_1] = ¾
Pr[**K**=k_2] = ¼

Note: Pr[Y=P] + Pr[Y=Q] + Pr[Y=R] = 1

CR

8

$$\Pr[x\mid y]=\frac{\Pr[x]\times\Pr[y\mid x]}{\Pr[y]}$$

plaintext	ciphertext
Pr[**X**=a] = 1/2	Pr[**Y**=P] = 1/6
Pr[**X**=b] = 1/3	Pr[**Y**=Q] = 3/8
Pr[**X**=c] = 1/6	Pr[**Y**=R] = 11/24

Pr[y|x]
Pr[P|a] = 0 Pr[P|b] = 0 Pr[P|c] = 1
Pr[Q|a] = ¼ Pr[Q|b] = ¾ Pr[Q|c] = 0
Pr[R|a] = ¾ Pr[R|b] = ¼ Pr[R|c] = 0

Pr[a|P] = 0	Pr[b|P] = 0	Pr[c|P] = 1
Pr[a|Q] = 1/3	Pr[b|Q] = 2/3	Pr[c|Q] = 0
Pr[a|R] = 9/11	Pr[b|R] = 2/11	Pr[c|R] = 0

If the attacker sees ciphertext ***P*** then she would know the plaintext was ***c***
If the attacker sees ciphertext ***R*** then she would know ***a*** is the most likely plaintext

---

K3

12. Consider the shift cipher, but with the following distribution over M:
$\Pr[M=kim]=0.5, \Pr[M=ann]=0.2, \Pr[M=\text{prove } boo]=0.3$ Solve the problem and compute the probability for $C=DQQ$?
Also prove or Refute: For every encryption scheme that is perfectly secret it holds that for every distribution over the message space M, every $m, m^1 \in M$and every $c \in C$: $\Pr[M=m \mid C=c]=\Pr\,[M=m' \mid C=c]$.

Answer

What is the probability that $C = \texttt{DQQ}$? The only way this ciphertext can occur is if $M = \texttt{ann}$ and $K = 3$, or $M = \texttt{boo}$ and $K = 2$, which happens with probability $0.2 \cdot 1/26 + 0.3 \cdot 1/26 = 1/52$.

We can also compute the probability that $\texttt{ann}$ was encrypted, conditioned on observing the ciphertext $\texttt{DQQ}$? A calculation as above using Bayes' Theorem gives $\Pr[M = \texttt{ann} \mid C = \texttt{DQQ}] = 0.4$. ◊

CO2

1.3.1
13.3.1

<table>
<tr>
<td></td>
<td>The proof is straightforward, but we go through it in detail. The key observation is that for any scheme, any distribution on M, any $m \in$ M for which Pr[$M = m$] > 0, and any $c \in$ C, we have

$$\Pr[C = c \mid M = m] = \Pr[\mathrm{Enc}_K(M) = c \mid M = m]$$
$$= \Pr[\mathrm{Enc}_K(m) = c \mid M = m]$$
$$= \Pr[\mathrm{Enc}_K(m) = c],$$</td>
<td></td>
<td></td>
</tr>
<tr>
<td colspan="4" align="center">OR</td>
</tr>
<tr>
<td>K3</td>
<td>13. Alice wants to send a message M with a message authentication code MAC(M) to Bob. Alice and Bob share a secret key k and have agreed on using a specific algorithm MAC function which takes input parameters M and k to produce MAC(M).
a. Apply the MAC algorithm and outline the steps that Alice must follow for sending M and the steps that recipient Bob must follow for verifying the authenticity of M.
b. Make of use the principle of MAC and explain why the MAC proves to Bob that a received message is authentic, and why Bob is unable to prove to a third party that the message is authentic.
Answer
a. MAC generation by Alice:
i. Alice prepares message M.
ii. Alice applies the secure algorithm MACfunc with input parameters M and k to produce MAC(M) = MACfunc(M,k).
iii. Alice transmits message M and MAC(M) to Bob, together with her unique name and specification of the MACfunc algorithm she used.
b. MAC validation by Bob:
i. Bob receives message M' (denoted as M', not M, because from Bob's point of view the message origin is still uncertain), as well as MAC(M).
ii. Bob applies MACfunc on M' to produce MAC(M') = MACfunc(M',k).
iii. Bob checks whether MAC(M) =? MAC(M'). If TRUE, then MAC(M) is valid, meaning that M' = M. Bob therefore is convinced that Alice really is the sender of message M. If FALSE, then the signature MAC(M) is invalid, meaning that M' ≠ M. Bob therefore does not know who created the received message M'. He might then decide to reject the message, or alternatively he can use it while knowing that its origin is uncertain.</td>
<td>CO2</td>
<td>1.3.1
13.3.1</td>
</tr>
</table>
