Case Study

Zodal Corporation have implemented a new voicemail system (VmS) for their staff. When a staff member X is away from their desk and their phone is unattended, the calling party is offered an option to record a voice message. VmS then sends an email to X about the missed call, and the message recording (if any) is attached to the email.

Question Group A

1. For the given case study, identify and discuss a possible threat against confidentiality. Be specific to the case study!
   Secondly, propose a security measure against that threat.
2. Encrypt the word MASTER using keyword TIE, according to Vigenère cipher. Show workings.

[4 + 2 + 4 marks]

Question Group B

1. For the given case study, discuss how you could apply the following principles to improve system security: least privilege and psychological acceptability. Give specific examples relevant to this system.
2. Perform a Railfence encryption of plaintext MESMERIZING using a depth of 4. Show workings.
3. How would an attacker be able to crack this ciphertext?

[3 + 3 + 2 + 2 marks]

Group A

Q2

plaintext	M	A	S	T	E	R
key	T=19	I=8	E=4	T=19	I=8	E=4
ciphertext	F	I	W	M	M	V

Group B

Q2

```
M-----I----    = MI
-E---R-Z---    = ERZ
--S-E---I-G    = SEIG
---M-----N-    = MN
```

Combined ciphertext: MI ERZ SEIG MN

Q3

Without knowing the key, attacker could manually try to rearrange the letters, or try railfence decryption with different depths.

Frequency analysis will only indicate that it is a transposition cipher, it will NOT provide any further help.