Name - Sradha Kedia
Roll no. - 20234757053
Subject - Information Security

Ans.f. ② (f) None of the Above

Reason: Jack and Jill both needs to have a mechanism to identify the other person's message and hence they need to Authenticated to do so i.e. need to be verified to identify the message.

The message sent by Jack is to be understood by Jill and vice-versa thus its need to be confidential i.e. to ensure the protection of data by preventing the unauthorized disclosure of information

third thing is any alteration during transmission must be detected by both thus pointing to Integrity part i.e. the data must not be changed or must not be altered and if so, the communicator must know about it.

The order is Authentication, Confidentiality, Integrity.

⑤ Plain Text : ATTACK POSTPONEDUNTILJANUARY

1	2	3	4	5	6	7	8	9
A	T	T	A	C	K	P	O	S
T	P	O	N	E	D	U	N	T
I	L	J	A	N	U	A	R	Y

— ①

The above matrix was made based on ciphertext
STYONRPNAKDUCENANATOJTPLATI

so, we can observe it starts with S, we write it of in vertical order S ; T, Y both are after S
T
Y

in Plaintext but O is before ensuring rows to be of three size; now, continuing this way O will be a column before S, O S ; we can realize we
N T
R Y

are going right OS is part of post, NT ~~of~~ until and RY of January. following the pattern we got ①, the matrix.

now they key according to ciphertext would be

$\boxed{987654321}$

Date

Page

① Vigenere cipher is a form of polyalphabetic cipher substitution.

~~S~~	~~T~~	~~A~~	~~Y~~	~~A~~	~~T~~	~~H~~	~~O~~	~~M~~	~~E~~	~~F~~	~~O~~	~~R~~	~~T~~	~~W~~	~~E~~	~~N~~	~~T~~	~~Y~~	~~O~~	~~N~~	~~E~~	~~D~~	~~A~~	~~Y~~	~~S~~
~~18~~	~~19~~	~~0~~	~~24~~	~~0~~	~~19~~																				

Plaintext:	S	T	A	Y	A	T	H	O	M	E	F	O	R	T	W	E	N	T	Y	O	N	E
P_i	18	19	0	24	0	19	7	14	12	4	5	14	17	19	22	4	13	19	24	14	13	4
Key:	S	R	A	D	H	A	S	R	A	D	H	A	S	R	A	D	H	A	S	R	A	D
K_i	18	17	0	3	7	0	18	17	0	3	7	0	18	17	0	3	7	0	18	17	0	3
C_i:	10	10	0	1	7	19	25	5	12	7	12	14	9	10	22	7	20	19	16	5	13	7
Ciphertext:	K	K	A	B	H	T	Z	F	M	H	M	O	J	K	W	H	U	T	Q	F	N	H

Plaintext:	D	A	Y	S
P_i:	3	0	24	18
Key:	H	A	S	R
K_i:	7	0	18	17
C_i:	10	0	16	9
Ciphertext:	K	A	Q	J

final ciphertext: KKABHTZFMHMOJKWHUTQFNH KAQJ

③ DES depends on key and rounds both. The larger the number of round the more secure it is because each round uses the matrix ~~to~~ (Substitution box) and hence more and more safer because of more confusion and difusion. And the keys also as we take larger key size we need to convert it into 48 bit thus more and more permutation compression thus more security is provided. It becomes difficult to decrypt if we use this both techniques in DES.

Ans ④ (b) 22160 mod 40702

i.e. we find gcd of 22160 & 40702.

gcd(22160, 40702)

q	r_1	r_2	r	
1	40702	22160	18542	
1	22160	18542	3618	gcd (22160, 18542)
5	18542	3618	452	gcd (18542, 3618)
8	3618	452	2	gcd (3618, 452)
226	452	2	0	gcd (452, 2)

in Euclidian Algo.

if gcd(a, b) = r then ∃ p and s

s.t. $p(a) + s(b) = r$

∵ the remainder is not equal to 1, ∴ Multiplicative inverse doesnot exist