(1) Show with a counterexample that the Substitution Cipher doesn't provide: perfect secrecy. PLAINTEXT: THE QUICK BROWN FOX. CIPHERTEXT: QEB NREZHYOLTK GUU different combination that need to be checked test case: A -B NO SECRECY K not decrypted Luck and it was been been all as THE QUICK BROWN FOX A TED P1, P2 = one-time pads C= ciphertext M = PlaintextC=M & P1 & P2 <sup>2</sup> cipheticxt One time pad is perfectly secret, because combination is used once. Alice encrypts: Bob Decrypts: Given: C=MOP1 DP1 D(c) = C & Py &R M= 101101 P1= 001001 C> 000000 M - 101101 P2= 100100 P1 - 001001 P1 > 001001 100100 001001 P2 -> 100100

C7 000000

P2 -7 10010 0

decrepted

Eve cannot intercept themessage unless She knows both pads

3.). ( 7167 K.)	house early 2.	Add hidle and die	a si kamban bi a sa pa saina	brids bridge ( hid not idea )	, d4 . a . 1	. Ú.
1. Han a	ittacker knows	a plaintex	t/cipher pair th	ey will know	what is store	d
in the o	latabase when the	y see an e	ncrypted cipher.	To the second of	,	
L	Fv. Fue has d	lanta in along	- has that though	Myo dialo		M Mar and the
. v kerre bekel . 1 . 1 11 11 11	which other	s the cipner or people hav	pose that they he positive the diabet	es plaintext	and canid	ar on thirty
£	prainty	J	ico prime presun	seeg. II 37	ke kegus e	nown
alı cip	ther text can be	decrypted.	ted withe the san	isk in Bell Augus in Anne on teach	·	ncwn
alı cip	ther text can be	decrypted.	L. I Aman	isk in Bell Augus in Anne on teach	·	10 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
au cip	ther text can be	decypied.	L. I Assist	isk in Bell Augus in Anne on teach	·	1000
au cip	ther text can be	decypred.	L-1 N 2 1 7 1 1	isk in Bell Augus in Anne on teach	·	nown
alı cip	ther text can be	decypred.	L. I Alexandra	isk in Bell Augus in Anne on teach	·	n Cwh

Brist a service of the fi

Tanto Later