HWI

tamen en venne de men en de formande en men Margaria samen mente en de de	Problem 2	
paginana dengani namina misima misima		and the contract of the contra
onkinnilis kulturi shari iyandari izanayini izanayili ili ili ili ili ili ili ili ili ili	If the key is indeed shared, then r will in	
	fact equal y.	of the state of th
	- Through eavesdropping, an attacker can gather what	
	both x and y are, since those are the messages that que know from step 3), that y = kb (X Through	re transmitted
	We know from step 3), that y=kb(+) X [through	1 the network
and an extransion of the contrast of the contr	- By using math, XORing y and X would be	graphy (s) (n) standigetaen shift of the ment of the standard measurement, compate the
and the section of th	equivalent to X XOR(X+K)	ga gapanan yang ang a spila gili sajik Salawan magai sapik sapikan na ang kana kana kana kana kana kana
	- That would leave us with the key	ikan kanada samiya panga panin nyaét terdinik katalanan nongé terdakitay da
		k symmetrikassy eight og friksjoher og i tre i tryspy eink og fri gyd eist opt optisk e kry
	$X \oplus Y = X \oplus (K_B \oplus X) = (X \oplus X) \oplus K_B = K_B$	
erministratus programitativos programinas programas sectors		and as fire following a resolver figure expension of the contract for the contract for figure figure.
	Example - Let's assume that the key is MOHO	
	- Alize generates r as [1011]	gradient format production and production and the contract of
and the state of t	-Therefore, X is calculated as 10 10 1011	langs y sinn tandige ngol, an a samati princy d (poly orthy o tay of trajence on careful of severant traject
	- Calculating y with the same key and x hould revel	L que quiem casaque, castaque depremensas, especimiente contensión de la compresión con es
meller mirk men stammenhend præte som stj. sperge priksense søre		The same of the sa
	- The hacker can then XOR x and y to return [1]	0/1/0/
R		
	it is all too possible to gain possession of the shared k	ey,
		an and makes the proof of the first of the second participates of the second of the se
	-If a hacker was able to modify any of the messeg	95,
	it nould be incredibly easy to make Alice and Bob	
	believe they don't share the same key.	
	- by XORing either X or y with 2"-1, where	eljelinis teoritusisionistaminista minerkistiministisi, atampi kaskunaksinnissa vuotei vuonna
	n is the amount of bits, the message's Os and Is	and the state of t
	would be inverted,	S
	- Therefore, that nould be how the attacker auld fool	agadamanian-ismining tamil
	Alice and Bob into believing they do not share the	
	same key.	reflective complete a consist of the costs, according to the printed an incidence according to