	name	MILCO (2014)	Bob (Receiver)			
	Drabi c leging		K̄8(n,e) =(35, 29) K̄β(n,e) =(35, 5)			
	2)Hash Function	11/12	H(x) = x mod 13			
	3)Symmetric Keying	-	How to get it?			
'\	4)Message		How to get it?			
	Alice (sender):					
	Step#	Description				
	1	Getmessage m -D M=17				
	2	Hash message - DH(m)=17%13=4				
	3	Encrypt Hashed message - 24d modn=42+%55=49				
	4	Encrypt Hashed message -124d modn=42t %55=49 Integrate W/ digital signature -> [17 [49]				
	5	Consorte Summetric Verito VS = 5				
	6	6 Encrypt rey w/ Boh's public rey: 5 mod 35 = 10				
	7	Encrypt message from 4 w/1cey: 122 54				
	8	Integrate with encrypted msg: Ks(m) Ks[Ka(Hcm)] ks(ks)				
	4		22	54 10		
	9	Send Step 8	's result to Bo	ob		
	THE STATE OF THE PROPERTY OF T					
	414444	Receiver (Bob				
	1	1 Receive data from alice: [22] 54 10				
	2	Split session key/message: 22,54 [10] Decrypt Megw/ session key: 17/49				
	3	Decryp+Msgw/ \$ 15 (10)=10 % 35=5				
	4	4 Decrypt Msg w/session key: 17/49				
	5	SPIH Msg & D5: 17, 49				
	6	Hash Msg: 17% 13=[4]				
	7 Decrypt Signature WAlice's Rublic Key: Pt (55,3) -> 493 mod 55=41					
	8 Compare hashes from 6 &7: 4=4; they're equal					
	9 If hashes are equal, msg is okay: Pass integrity check; msg=okay					
10	C Long L CKAKEY					
4)	Sender Side (Kakey) M-D/H(.) HKa(.) HKa(Hcm)) KS					
	MI-DIH(0) FIKA(0) T					
-	V V					
_	4) - 1/K2(.)					
	M Sent content?					
	KZ MYB() KB(KS)					
	Buch					
A CHARLES CONTRACTOR OF THE PARTY OF THE PAR	4.500	Marine the selection of the security of the se				

