3.8 Keyed Harh - Jo tha the file a he hashed with some secret key. 3.9 Morble: Pazzle 9(cp): Generate 128 bit keys. 125 bit keys: Pazzle 9(cp): Generate 128 bit keys. 125 bit keys: Pazzle 9(cp): Generate 128 bit keys. 125 bit keys: Pazzle 9(cp): Generate 128 bit keys. 126 bit keys: Pazzle 9(cp): Generate 128 bit keys. 127 Es; (bi, ki, hi, his): man secret keys: 128 Es; (bi, ki, his): man 128 Es; (bi, ki): man 128 Es; (3.8 Keyed Havin 2.10 this the file is be bashed both some secret hey. 2.11 bit heys: In. his his. ha for the file heys: Secret hey. 2.11 bit heys: In. his his. ha for secret hey. Superior succeeding high so bit hey was creeypt secret. Secret heys: An hold) - M. Esa (ta, k., h(h)) - M. Esa (ta, k., h(h)) - M. Superior she transmitted high so he to so he so he secret. Such: Bab roadonly pick a message his. Here: One has been fore to open the march his of and train his disconsisted here has to say for a time of and to so hos sides when he has to say for a time some fine march his his hay he attacked he has to say for a time some fine march his high his hay had gay have to cran a 244 If there can generate 236 mexages Attacker computational over heard: 244 If there can generate 236 mexages Attacker computational over heard: 245 If there can generate 236 mexages Attacker computational was heard. If there is need 256 secrets to crack, how by his hay have 2 too accords. Block 5 - Randon Mumbers. Dual Energyphian: In was superior a server of the history pick message marks to the history of the history pick in his high history is superior to the history pick message marks to the history of the history pick in history is superior to the history pick in history is superior to the history of the history pick in history is superior to the history of the history pick in history is superior to the history of the history pick in history is superior to the history pick in history in history pick in history is superior to the history pick in history in in	3-9.pdf 939.3 KB	ad. (a) 💿 🛂
Jo that the file is he bashed with some secret hey. 3.9 Movble's Puzzle 2tcpl: Generate 128 bit keys. 121 bit keys: In. 122 his. 123 sh. 6h bit keys: In. 122 his. 123 sh. 5h bit keys: In. 122 his th. 4102! 81	Sign that the file a has bashed with some secret heap. Sign Markley Puzzle Step 1 General 128 bit keys. In his file In 131 bit heys ? 108 bit keys. In his secret hey! She bit heys ? 108 bit keys. In his secret hey! Sucrete summerice Agg six bit key used concepts secrete beet 1, k, h(h) ? Mi Fis (ta, ka, h(h)) * Mi Fis (ta, ka, h(h))		
Jo that the file is he bashed with some secret hey. 3.9 Movble's Puzzle 2tcpl: Generate 128 bit keys. 121 bit keys: In. 122 his. 123 sh. 6h bit keys: In. 122 his. 123 sh. 5h bit keys: In. 122 his th. 4102! 81	Sign that the file a has bashed with some secret heap. Sign Markley Puzzle Step 1 General 128 bit keys. In his file In 131 bit heys ? 108 bit keys. In his secret hey! She bit heys ? 108 bit keys. In his secret hey! Sucrete summerice Agg six bit key used concepts secrete beet 1, k, h(h) ? Mi Fis (ta, ka, h(h)) * Mi Fis (ta, ka, h(h))		
21cpl: Generate 178 bit keys. 21cpl: Generate 178 bit keys. 12s bit keys = 141, 162, 163, kn. 64 bit keys = 161, 162, 163, sn. 64 bit keys = 161, 162, 163, sn. 64 bit keys = 164 bit key used encrypt 64 Es, (t, k, h(k)) = 161 65 Es, (t, k), h(k) = 161 65	Attacker Competitions over head: 20 Markler Pazzlo 21 Markler Pazzlo 21 Markler Pazzlo 22 Markler Pazzlo 23 Markler Pazzlo 24 Markler Pazzlo 25 Markler Maga Shist Reg mad energet 25 Markler Maga Shist Reg mad energet 25 Markler Maga Shist Reg mad energet 26 Markler Markler Markler Markler Pazzlo 26 Markler Markler Markler Markler Markler 21 Markler Markler Markler Markler 26 Markler Markler Markler Markler 26 Markler Markler Markler 26 Markler Markler 27 Markler Markler 28 Markler Markler 29 Markler 29 Markler 20 Markler 20 Markler 20 Markler 20 Markler 20 Markler 20 Markler 21 Markler 22 Markler 23 Markler 24 Markler 24 Markler 25 Markler 26 Markler 26 Markler 27 Markler 28 Markler 29 Markler 20 Markler 21 Markler 22 Markler 23 Markler 24 Markler 25 Markler 26 Markler 26 Markler 27 Markler 28 Markler 29 Markler 20 Markler 26 Markler 27 Markler 28 Markler 28 Markler 28 Markler 28 Markler 28 Markler 28 Markler 29 Markler 29 Markler 20 Markler		
3.9 Markles Puzzle Stepl Generate 128 bit keyk. 121 bit keys = 101, 102 103 kn. 64 bit keys = 101, 102 103 kn. 64 bit keys = 101, 102 103 kn. Stepl Segment of the test is the segment of the test is the segment of the segment o	Attacker Competitions over head: 20 Markler Pazzlo 21 Markler Pazzlo 21 Markler Pazzlo 22 Markler Pazzlo 23 Markler Pazzlo 24 Markler Pazzlo 25 Markler Maga Shist Reg mad energet 25 Markler Maga Shist Reg mad energet 25 Markler Maga Shist Reg mad energet 26 Markler Markler Markler Markler Pazzlo 26 Markler Markler Markler Markler Markler 21 Markler Markler Markler Markler 26 Markler Markler Markler Markler 26 Markler Markler Markler 26 Markler Markler 27 Markler Markler 28 Markler Markler 29 Markler 29 Markler 20 Markler 20 Markler 20 Markler 20 Markler 20 Markler 20 Markler 21 Markler 22 Markler 23 Markler 24 Markler 24 Markler 25 Markler 26 Markler 26 Markler 27 Markler 28 Markler 29 Markler 20 Markler 21 Markler 22 Markler 23 Markler 24 Markler 25 Markler 26 Markler 26 Markler 27 Markler 28 Markler 29 Markler 20 Markler 26 Markler 27 Markler 28 Markler 28 Markler 28 Markler 28 Markler 28 Markler 28 Markler 29 Markler 29 Markler 20 Markler	-> In the the file is be hashed with some secret key.	
Secrete key: For Es, (t, k, h(k)) = m, Esa (ta, ka. h(ka)) = mn Steps: Belie mia dump MMo to Bob. Steps: Bob randomly pick a munage M?, steps: Bob best brute free to open the wing all legs. Now both sider will know ki. (IMM 1) ->if the attacker wants to open the matru the menage he how to try for n times time ruere are n menuages a 14 bit key i. bod gay how to crack n.264 bob tour to crack 264 -> If Alice can generate 236 messages Attacher Computation over heard: 236. 264e -> If Bob need 236 securels to crack, Rad genys have 2 loo records. Black 5 - Random Mumbers. Dual Eneryption;	Scients key (1, k, h (k)) = m. Scients key (1, k, h (k)) = m. Esa (ta, ka, h (k)) = m. Step3: with a wire dump M Mo to 80h. Step4: Bob trandomy pick a mescage N? Mep 5: hos the but fore to mescage N? Mep 6: not fore to the fore the mescage N? Now 6on sode to the how hi. (Infly 1) -> 21 Me attracter worth to open the march the names of he has to try for 1 three -> 10 May 1) -> 21 Me attracter worth to open the march the names of he has to try for 1 three -> 10 May 1 how to crock n. 244 -> 14 Attocker Computation over head: Q26. 264 -> 15 Bob need Q36 scients to crock, Roo by any hove 2 too (ccords.) Block B - Random Numbers. Dual Encryption: (a) Block B - Random Numbers. Dual Encryption: (b) bit ky: S152 - Sn message M? Esa (t1, k1, h(k))=M2 A, I choose t; atk Mi Esa (t1, k1, h(k))=M1 Limpoption		
Secrete key: Secrete key: For Es, (t, k, h, h(k)) = m, Esa (ta, k2, h(k2)) = m, Esa (ta, k2, h(k2)) = m, Esa (ta, k2, h(k2)) = m, Sheps: Bob kan holding MMo to Bob. Sheph: Bob randomly pick a munage M?, Wep E: Bob hes brute fixe to open the wing all heys: Now born sider work for Active. Now born sider work know hi. (I'my 1) -> if the attacker wants to open the match the menage he how to try for notimes cince menage he how to try for notimes cince menage he how to crack not be bob key bob key to chack 264 -> If Alvice can generate 236 messages Attacher Computation over heard: 236. 264e 2100 i. If Bob need 236 seconds to crack, Rad beguy have 2 loo records. Black 5 - Random Mumbers. Dual Encryption;	Scients key (1, k, h (k)) = m. Scients key (1, k, h (k)) = m. Esa (ta, ka, h (k)) = m. Step3: with a wire dump M Mo to 80h. Step4: Bob trandomy pick a mescage N? Mep 5: hos the but fore to mescage N? Mep 6: not fore to the fore the mescage N? Now 6on sode to the how hi. (Infly 1) -> 21 Me attracter worth to open the march the names of he has to try for 1 three -> 10 May 1) -> 21 Me attracter worth to open the march the names of he has to try for 1 three -> 10 May 1 how to crock n. 244 -> 14 Attocker Computation over head: Q26. 264 -> 15 Bob need Q36 scients to crock, Roo by any hove 2 too (ccords.) Block B - Random Numbers. Dual Encryption: (a) Block B - Random Numbers. Dual Encryption: (b) bit ky: S152 - Sn message M? Esa (t1, k1, h(k))=M2 A, I choose t; atk Mi Esa (t1, k1, h(k))=M1 Limpoption	Step 1: Generate 128 bit keys, 128 bit keys = 121, 12, 123, 12n.	
Scerck key: Secrete key: For Es, (t, k, h(k)) = mi Esa (ta, ka, h(k2)) = mi Esa (ta, ka, h(k2)) = mi Steps: Belie wire dump Mi Mo to Bob. Steph: Bob randomly pick a murage M?, MEP E: Bob was brake force to open the wing all Next of Bob opens mency and choose seq the and work to Alie. Now both sider work know ki. (I'my 1) ->if the attracter wants to open the march the manage he how to try for n times since mere are n mency ses & 14 bit key i. bad gay how to chack n.244 bob tour to chack 264 -> If Alice can generate 236 messages Attacher computations over heard: 236. 264e -> 2100 i. St. Bob need 236 secureds to crack, Rad genys have 2 loo records. Block 5 - Random Mumbers. Dual Eneryption;	Scients key (1, k, h (k)) = m. Scients key (1, k, h (k)) = m. Esa (ta, ka, h (k)) = m. Step3: with a wire dump M Mo to 80h. Step4: Bob trandomy pick a mescage N? Mep 5: hos the but fore to mescage N? Mep 6: not fore to the fore the mescage N? Now 6on sode to the how hi. (Infly 1) -> 21 Me attracter worth to open the march the names of he has to try for 1 three -> 10 May 1) -> 21 Me attracter worth to open the march the names of he has to try for 1 three -> 10 May 1 how to crock n. 244 -> 14 Attocker Computation over head: Q26. 264 -> 15 Bob need Q36 scients to crock, Roo by any hove 2 too (ccords.) Block B - Random Numbers. Dual Encryption: (a) Block B - Random Numbers. Dual Encryption: (b) bit ky: S152 - Sn message M? Esa (t1, k1, h(k))=M2 A, I choose t; atk Mi Esa (t1, k1, h(k))=M1 Limpoption	Scoprene # = t, t2, t3 In.	
Steps: Allie w'u dump M Mn to Bob. Steps: Allie w'u dump M Mn to Bob. Steps: Bob was but fire to open M. wing all Reys. Steps: Bob was but fire to open M. wing all Reys. Now both sides will know hi. (Imy 1) -> If the atracker wents to open the march the menage he how to try for n times Kime menage he how to try for n times Kime these are n menuses & 64 bit key bob tem to chack ~ 254 -> If Alice lan generate 236 menages Attacker Computation over head: 236. 264 = 2100 If Bob need 236 seems to crack, Rad begange have 2 loo seconds. Blak B - Random Mumbers. Dual Encyption;	Step3: selie wire dump Mi. Mo to Bob. Step3: selie wire dump Mi. Mo to Bob. Step4: Beb translandy pick a manage Mf. The G. Beb come manage and dworse say to and and to Mile. Now Both solve weath to open the march the unrange wants to open the march the unrange wants to the form the solve they the unrange of the both to the form the march the unrange of the both to the form they since Male are a mencases of the bit key bod gay how to chack n.2644 bit but to chart 244 The Alrice can generate 236 menages Attacker computations over head: 231. 964e 2100 Step Bob need 236 records. Block 5 - Random Mumbers. Dual Encryption: Charter the form overhead for computation Overhead: Encryption: M. M2. Ma randomly pick appearate many k, ks ma generate the form overhead for computation overhead: Encryption: Sequence the tite - to sequence the mile of the tite of the tite the both to the second of the tite of the tite sequence the tite - to sequence the tite - to sequence the tite - to sequence the tite of the tite of the tite the both tite of the tite the both tite of the tite of the tite the both the second the second the second the second the tite of the tite the tite of the tite of the tite of the tite of the tite the tite of the ti	select summethic Algo 64 bit key he con craige	At .
Steps: Addie wir dump MyMo to Bob. Sterki: Bob mandomy pick a mercage M?. Mep 5: Bob was bruse free to open My wing all Mays. Men 6: Bob opens mercage and choose see ti and sends to Acie. Now both sider wire know hi. Cimy 1) if the attracker wants to open the march the menage he how to try for n time since mere are n mercases & 64 bit key bod gay has to crack N. 264 bob how to crack 264 -> If Alice can generate 236 mercages Attacker computation over head: 236. 264 2100 i. If Bob need 286 security to crack, Rad genys have 2 loo records. Black 5 - Random Mumbers. Dual Encryption:	Step 3: Attile will during My He to 806. Step 1: Beb to productly pick a menage N. 1. Mr P S Deb there but the pick to open M. 1. Mr P S Deb there but the first to open M. 1. Mr P S Deb there but the first to open the march to be step to be step to the know bi. (I'my 1) -> 2] the attractor wants to open the march the menage he has to try for n time time there are menages of 14 bit key. -> It Alive Lan generate 236 menages Attacker competitution over heard: 236, 264; -> 100 -> 14 Alive Lan generate 236 menages Attacker competitution over heard: 236, 264; -> 100 -> 15 Bob need 236 remale to crack, Roo gery have 2 too 100 ccools. Block 5 - Random Mumbers. Dual Encryption: What try to establish a key 128 bit key. Brande communication aerhead for computation over heard. Converted (converted (conv	Est Est (t, , K, , h(k2)) = M2 Esa (ta, k2, h(k2)) = M2	
Steph: Bob randomly pick a merage No. Step 5: Bob was brute free to open Wi curing all beys: Bob was brute free to open Wi curing all step 6: Bob opens mexicus and choose sog ti and sends to Allie. Now both sides with know hi. (IMY 1) -> If the attracter wants to open the match the menage he how to try for n times since these are n menages & 4 4 bit key -> Dad gay how to crack N. 264 bob how to crack 264 -> If Alice Lan generate 236 mexages Attacher Computations over head: 236. 264 -> If Bob need 236 secures to crack, Rad gerys have 2 loo secures. Black 5 - Random Mumbers. Dual Eneryption:	Steph: 86 prodomoty pick a mercage NT. The First Dose was busted fine to reach NI ways are least. The of all opens making and choose reach the of all opens making and choose reach Now both eider when he file. Now both eider wasts to open the mateur the mennage he has to try for n dime time release are a mercage of 14 bit key that gay has to crack n. 244 bob how to chast 244 The Alive is a generate of mercages Attacker competations over heard: Q25. 264 2 100 The Bob need of secures to crack, Roo of geny have a loo records. Black 5 - Random Mumbers. Dual Eneryption: Min M2. The waste many k, ks. for mercage min message min secure to the key; S 52. The both key; S 52. The message min respective to the key of the key; S 52. The both key; S 52. The message min respective to the key of the key; S 52. The both key; S 52. The message min secure to the kind of the message min secure to the key; S 52. The sequence to the kind of the kin		
ster 6: Bob opens mexcuge and choose seg to and serbs to Ashe. Now both sides will know hi. (IM) 1) -> if the attacker wants to open the march the mexage he how to try for notines since these are nomenages of 64 bit keep in bad guy how to chack not be then to chack 264 -> If Alice can generate 236 mexages Attacker Computation over heard: 236. 264 = 2100 If Bob need 286 secures to crack, Rad genys have 2 loo seconds. Black 5 - Random Mumbers. Dual Eneryption:	Free G. B.th open manage and choose son to act to act to be seek sold to be the sold to the file. Now both scold sold know hi. - If the attractor wants to open the march the march the manage he had to try for n times since these one in memory. I had gay how to crack n. 264 - If Alice can generate 236 memages Attacker computations over heard: 231. 264 - 2100 - If Bob need 236 secureds to crack, Race genys have 2 loo seconds. Black 5 - Random Mumbers. Dual Encryption: What they is seen to memory the sold service to crack, Race genys have 2 loo seconds. Black 5 - Random Mumbers. Dual Encryption: Kith they keep to see the sold for computation over heard. Sold bit key: s. s. s Sn M. M2 Mn Enarched the sold seen to the sold process of the sold seen to the sold se	Step 3: Active min dump Mi Mr. 10 805, Step 4: Bob randomly pick a message M?, step 5: Bob was brute force to open Mi wing all	
Now both sides will know hi. (jong) -> if the atracker wants to open the march the menage he how to try for n times since there are n menages & 64 bit key bod gay how to chack n. 264 -> If Alice Lan generate 236 mexages Attacher Computations over head: 236. 264 -> 100	Now both sides with know hi. (IM) 11 ->21 the attacker wants to open the march the memory he have to try for n time since men care a memory he has to try for n time since men care and memory has been not been	lexus.	
the menage he has to try for notimes since there are no menages & 64 bit key bad gay how to crack no 264 To Alice can generate 236 messages Attacher computations over head: 236. 264 = 2100 i. Sy Bob need 236 generals to crack, Rad genys have 2 loo seconds. Black 5 - Random Mumbers. Dual Eneryption:	the mestage he has to ry for no many fine rene are no mencages of the bit key is but gay how to chack n. 264 bot her to chack 264 bot h	Now both sides will know hi.	
the menage he has to try for notimes since there are no menages of 4 bit key bad gay how to chack no 264 To Alice can generate 236 messages Attacher computations over head: 236. 264 = 2100 i. Sy Bob need 236 generals to crack, Rad genys have 2 loo seconds. Block 5 - Random Mumbers. Dual Eneryption:	the mestage he has to ry for no many fine rene are no mencages of the bit key is but gay how to chack n. 264 bot her to chack 264 bot h	-> If the atracker wants to open the mate	4
-> If Alive Lan generate 236 mexages Attacher Computation over head: 236. 264 = 2100 i. If Bob need 236 generals to crack, Rad genys have 2 100 records. Block 5 - Random Mumbers. 1) wal Eneryptian;	The Muice can generate 236 messages Attacker computations over head: 236, 264 2100 i. St. Bob need 236 seconds to crack, Rood by Love 2 loss records. Black 5 - Random Mumbers. Dual Encryptian: Lenarate many (k, k2-kn) M. M2 May requested for computation over head. (Ka) bit key: Si S2 Sn randomly pick message mi Esi (t1, k1, h(k1))=M1 Esi (t2, k2, h(k2))=M2 A, I choose ti atk Mi Esi (t2, k2, h(k2))=M2 A, I choose ti atk Mi (tn, kn, h(kn))=Mn A whoever	the menage he how to try for n time since there are n menages & 64 bit key in bad gay how to chack n. 264	હ
Attacher Computation over head: 236.264 = 2100 i. St. Bob need 236 seemels to crack, Rad genys have 2100 records. Block 5 - Random Mumbers. Dual Eneryption:	Attacker Computation over head: 236. 264 2 100 i. J. Bob need 236 seconds to crack, Rad begung have 2 100 seconds. Black 5 - Random Mumbers. 1) wal Encryption: trade communication overhead for computation over head generate many 28 bit key: (2) 52 - 5n sequence #: t, t, h(k) = M1 Esi (t, k, h(k)) = M2 Esi (t, k, h(k)) = M2 Kin Landowsky pick message mi Esi (t, k, h(k)) = M2 Esi (t, k, h(k)) = M2 Lincopption A whoever Response to crack, Rad Boute for computation randomly pick message mi Esi (t, k, h(k)) = M1 Esi (t, k, h(k)) = M2 Lincopption	bob hen to chack ~ 26	4
Attacher Computation over head: 236.264 = 2100 i. St. Bob need 236 seemels to crack, Rad genys have 2100 records. Block 5 - Random Mumbers. Dual Eneryption:	Attacker Computation over head: 236. 264 2 100 i. J. Bob need 236 seconds to crack, Rad begung have 2 100 seconds. Black 5 - Random Mumbers. 1) wal Encryption: trade communication overhead for computation over head generate many 28 bit key: (2) 52 - 5n sequence #: t, t, h(k) = M1 Esi (t, k, h(k)) = M2 Esi (t, k, h(k)) = M2 Kin Landowsky pick message mi Esi (t, k, h(k)) = M2 Esi (t, k, h(k)) = M2 Lincopption A whoever Response to crack, Rad Boute for computation randomly pick message mi Esi (t, k, h(k)) = M1 Esi (t, k, h(k)) = M2 Lincopption		
Attacher Computation over head: 236.264 = 2100 i. St. Bob need 236 seconds to crack, Rad genye have 2100 records. Black 5 - Random Mumbers. 1) wal Eneryptian:	Attacker Computation over head: 236. 264 2 100 i. J. Bob need 236 seconds to crack, Rad begung have 2 100 seconds. Black 5 - Random Mumbers. 1) wal Encryption: trade communication overhead for computation over head generate many 28 bit key: (2) 52 - 5n sequence #: t, t, h(k) = M1 Esi (t, k, h(k)) = M2 Esi (t, k, h(k)) = M2 Kin Landowsky pick message mi Esi (t, k, h(k)) = M2 Esi (t, k, h(k)) = M2 Lincopption A whoever Response to crack, Rad Boute for computation randomly pick message mi Esi (t, k, h(k)) = M1 Esi (t, k, h(k)) = M2 Lincopption		
i. If Bob need 236 seemels to crack, Rad genys have 2 loo records. Block 5 - Random Mumbers. Dual Eneryption:	is 5, 806 need 236 secunds to crack, Race Bey have 2 loo records. Black 5 - Random Mumbers. Dual Encryption: Trade communication overhead for computation over head. Separate many (2) Both to 1, 1/2 - 1/2 Both to 1, 1/2 - 1/2 Sequence #: 1, 12 - 1/2 Sequence #: 1, 12 - 1/2 Esi (t1, k1, h(k1))=M1 Esi (t2, k2, h(k2))=M2 A whoever	-> It Alice lan generate 236 m	renages
i. If Bob need 2 ³⁶ secures to crack, Rad gerye have 2 loo records. Block 5 - Random Mumbers. 1) wal Eneryption;	is 5, 806 need 236 secunds to crack, Race Bey have 2 loo records. Black 5 - Random Mumbers. Dual Encryption: Trade communication overhead for computation over head. Separate many (2) Both to 1, 1/2 - 1/2 Both to 1, 1/2 - 1/2 Sequence #: 1, 12 - 1/2 Sequence #: 1, 12 - 1/2 Esi (t1, k1, h(k1))=M1 Esi (t2, k2, h(k2))=M2 A whoever	Attacher Computation over head	236.264
Block 5 - Random Mumbers. 1) wal Eneryption:	Black 5 - Random Mumbers. Dual Eneryption: We trade communication are thead for computation over head: Benarate many k, k2 - kn m, m2 - mn Sequence t: t, tz - tn message mi Esi (ti, ki, h(ki))=Mi Esi (tz, kz, h(kz))=Mz Esi (tz, kz, h(kz))=Mz Esi (tz, kz, h(kz))=Mn Li ki h	= 2100	
Block 5 - Random Mumbers. 1) wal Eneryption:	Black 5 - Random Mumbers. Dual Eneryption: We trade communication are thead for computation over head: Benarate many k, k2 - kn m, m2 - mn Sequence t: t, tz - tn message mi Esi (ti, ki, h(ki))=Mi Esi (tz, kz, h(kz))=Mz Esi (tz, kz, h(kz))=Mz Esi (tz, kz, h(kz))=Mn Li ki h	i. I Rob need 236 exemples	o crack Dad
Block 5 - Random Mumbers. 1) wal Eneryption:	Black 5 - Random Mumbers. Dual Eneryption: We trade communication are thead for computation over head: Benarate many k, k2 - kn m, m2 - mn Sequence t: t, tz - tn message mi Esi (ti, ki, h(ki))=Mi Esi (tz, kz, h(kz))=Mz Esi (tz, kz, h(kz))=Mz Esi (tz, kz, h(kz))=Mn Li ki h	gerge have 2 los records.	, ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
Dual Eneryption:	A try to establish a key. 128 bit key. B trade communication overhead for computation over head. Jenarate many 28 bit key: \$1 \$2 - 5n 64 bit key: \$1 \$2 - 5n Sequence #: \$1 \$2 - 5n Fest (\$1, K1, h(K1))=M1 Est (\$1, K1, h(K1))=M2 A. I choose \$1 atk Mi Est (\$1, Kn, h(Kn))=Mn A whoever A Tencryption		
	trade communication overhead for computation over head. Jenarate many k, k2—kn m. m2 mn 28 bit kay: \$1, \$2 \$n 64 bit key: \$1, \$2 \$n Esquence #: \$1, \$2	Block 5 - Kandom Mumbers.	
	trade communication overhead for computation over head. Jenarate many k, k2—kn m. m2 mn 28 bit kay: \$1, \$2 \$n 64 bit key: \$1, \$2 \$n Esquence #: \$1, \$2	Dual Eneryption:	•
	trade communication overhead for computation over head. Jenarate many Replacement to the pick of the		
	trade communication overhead for computation over head. generate many (k) 28 bit key: (k, k2-16) 64 bit key: (s) 52 Sn (sequence #: t, t2tn (sequence #: t, t2tn (t1, K1, h(K1))=M1 Esi (t1, K2, h(K2))=M2 A. I choose ti atk Mi (tn, Kn, h(Kn))=Mn ti Ki h I encryption A whoever		
	trade communication overhead for computation over head. generate many (k) 28 bit key: (k, k2-16) 64 bit key: (s) 52 Sn (sequence #: t, t2tn (sequence #: t, t2tn (t1, K1, h(K1))=M1 Esi (t1, K2, h(K2))=M2 A. I choose ti atk Mi (tn, Kn, h(Kn))=Mn ti Ki h I encryption A whoever		
	trade communication overhead for computation over head. generate many (k) 28 bit key: (k, k2-16) 64 bit key: (s) 52 Sn (sequence #: t, t2tn (sequence #: t, t2tn (t1, K1, h(K1))=M1 Esi (t1, K2, h(K2))=M2 A. I choose ti atk Mi (tn, Kn, h(Kn))=Mn ti Ki h I encryption A whoever		
	trade communication overhead for computation over head. generate many (k) 28 bit key: (k, k2-16) 64 bit key: (s) 52 Sn (sequence #: t, t2tn (sequence #: t, t2tn (t1, K1, h(K1))=M1 Esi (t1, K2, h(K2))=M2 A. I choose ti atk Mi (tn, Kn, h(Kn))=Mn ti Ki h I encryption A whoever		
	trade communication overhead for computation over head. generate many (k) 28 bit key: (k, k2-16) 64 bit key: (s) 52 Sn (sequence #: t, t2tn (sequence #: t, t2tn (t1, K1, h(K1))=M1 Esi (t1, K2, h(K2))=M2 A. I choose ti atk Mi (tn, Kn, h(Kn))=Mn ti Ki h I encryption A whoever		
	trade communication overhead for computation over head. generate many (k) 28 bit key: (k, k2-16) 64 bit key: (s) 52 Sn (sequence #: t, t2tn (sequence #: t, t2tn (t1, K1, h(K1))=M1 Esi (t1, K2, h(K2))=M2 A. I choose ti atk Mi (tn, Kn, h(Kn))=Mn ti Ki h I encryption A whoever		
A la	genarate many (ki) 28 bit key: (ki, kz-kn) 64 bit key: (ki, kz-kn) Sequence #: (ti tz-tn) Mi M2 Mn randomly pick message Mi Esi (ti, ki, h(ki))=Mi Esi (ti, ki, h(ki))=Mi Esi (ti, ki, h(ki))=Mi Esi (ti, ki, h(ki))=Mn The choose to atk Mi Esi (ti, ki, h(ki))=Mn The choose to atk Mi		Le
	28 bit key: (k, k2-kn) M. M2 64 bit key: S1 S2Sn Sequence#: t1t2tn Message Mi Es1 (t1, K1, h(K1))=M1 Es1 (t2, k2, h(K2))=M2 A, I choose ti atk Mi Es2 (t2, k2, h(K2))=Mn (tn, Kn, h(Kn))=Mn ti Ki h Heneryption	Kin try to establish a key: 128 bit	
	28 bit key: (k, k2-kn) M. M2 64 bit key: S1 S2Sn Sequence#: t1t2tn Message Mi Es1 (t1, K1, h(K1))=M1 Es1 (t2, k2, h(K2))=M2 A, I choose ti atk Mi Es2 (t2, k2, h(K2))=M2 (tn, Kn, h(Kn))=Mn ti Ki h I Encryption	Kin try to establish a key: 128 bit	
	28 bit kay: Ki Ksantin Mi M2 64 bit key: Si SzSn Sequence#: titztn Message Mi Esi (ti, Ki, h(ki))=Mi Esi (tz, kz, h(kz))=Mz A, I choose ti atk Mi Esz (tz, kz, h(kx))=Mn Ti Ki h I atk Ti Ki Ki h I atk Ti Ki h I atk	Kig to establish a key: 128 bit	
trade communication overhead for computation over head.	Esi (t2, k2, h(k2))=1M2 A, I choose ti atk Mi Esz (t2, k2, h(k2))=Mn ti 64 bit (tn, kn, h(kn))=Mn ti ki h le A whoever	Ki trade communication overhead for overhead.	
trade communication overhead for computation over head.	Esi (t2, k2, h(k2))=1M2 A, I choose ti atk Mi Esz (t2, k2, h(k2))=Mn ti 64 bit (tn, kn, h(kn))=Mn ti ki h le A whoever	Ki try to establish a key: 128 bit trade communication overhead for overhead.	
trade communication overhead for computation over head.	Esi (t2, k2, h(k2))=1M2 A, I choose ti atk Mi Esz (t2, k2, h(k2))=Mn ti 64 bit (tn, kn, h(kn))=Mn ti ki h le A whoever	Ki try to establish a key: 128 bit trade communication overhead for overhead.	
trade communication overhead for computation over head. generate many (ki) 28 bit key: K1 K2-Kn) M. M2 Mn 128 bit key: S1 S2 Sn 64 bit key: S1 S2 Sn sequence #: t1 tz tn message mi	I Encryption Li (tn, kn, h(kn))=Mn ti (ti ki h) A Whoever	Ki try to establish a key: 128 bit trade communication overhead for overhead.	randomly pick message mi
trade communication overhead for computation over head. generate many (k) 28 bit ky: (k, k2-kn) M. M2 Mn 128 bit ky: (k, k2-kn) M. M2 Mn randomly pick sequence #: t1tztn sequence #: t1tztn Es (t1, K1, h(k1))=M1 Es (t1, K1, h(k1))=M1 A 7 choose to B brute force to	Auhoever	Ki trade communication are thead for over head. generate many (ki) 128 bit key: Ki K2-Kn M. M2 Mn 64 bit key: Si S2Sn sequence #: titztn Sequence #: titztn Ec (ti, Ki, h(ki))=Mi	randomly pick message mi
trade communication overhead for computation over head. generate many (k) 28 bit key: (k) 64 bit key: (s) 52	Auhoever	Ki trade communication are thead for over head. generate many (ki) 28 bit key: Ki K2-In M. M2 Mn 64 bit key: Si S2Sn sequence #: titztn Ec (ti, Ki, h(ki))=Mi	randomly pick message mi
trade communication overhead for computation over head. generate many (k) 28 bit ky: (k, k2-kn) M. M2 Mn 128 bit ky: (k, k2-kn) M. M2 Mn randomly pick message mi Sequence #: t1tztn sequence #: t1tztn Es (t1, K1, h(k1))=M1 Es (t1, K1, h(k1))=M1 A 7 choose to B brute force to	Auhoever	Ki trade communication are thead for over head. generate many (ki) 128 bit key: Ki K2-Kn M. M2 Mn 64 bit key: Si S2Sn sequence #: titztn Ec (ti, Ki, h(ki))=Mi	randomly pick message mi
trade communication overhead for computation over head. generate many (ki) 28 bit key: K, K2-Kn) M. M2 Mn 64 bit key: S, S2Sn sequence #: t, t2tn message mi Esi (t1, K1, h(K1))=M1 Esi (t2, k2, h(K2))=M2 Esi (t2, k2, h(K2))=M2 A, I choose ti atk Mi Esi (tn, Kn, h(Kn))=Mn ti Kih	A pub_A pub_A pub_A pub_B A,B. (Signpial Epub_B (MSg)) A,B (Epub_B) (Signpia (Msg)) Bob	Kit trade communication overhead for overhead. generate many (ki) 128 bit key: K, K2-Kn) M. M2 Mn 64 bit key: S, S2Sn sequence#: t, tztn Esi(t1, K1, h(k1))=M1 Esi(t2, k2, h(k2))=M2 A, I choose ti Esi(tn, Kn, h(kn))=Mn	randomly pick message mi
trade communication overhead for computation over head. generate many (ki) 28 bit key: K1 K2-Kn) M. M2 Mn 64 bit key: S1 S2Sn sequence #: t1 t2tn message mi Es1 (t1, K1, h(K1))=M1 Es1 (t2, k2, h(K2))=M2 Es2 (t2, k2, h(K2))=M2 A, I choose ti atk Mi Es2 (tn, Kn, h(Kn))=Mn ti Kih	pub_A pub_A pub_B SignpiA Epub_B Signpia (Msg) Bob	Ki trade communication overhead for over head. generate many (ki) 128 bit key: Ki K2-kn M. M2 Mn 64 bit key: Si S2Sn sequence #: titztn Ec (ti, Ki, h(ki))=Mi	randomly pick message mi
trade communication overhead for computation over head. generate many (ki) 28 bit key: K1 K2-Kn) M. M2 Mn 64 bit key: S1 S2Sn sequence #: t1t2tn message mi Es1 (t1, K1, h(K1))=M1 Es1 (t2, k2, h(K2))=M2 Es2 (t2, k2, h(K2))=M2 A, I choose ti atk Mi Es2 (tn, Kn, h(Kn))=Mn ti Kih	Pub_B SignpiA (Mg) Pub_B Signpia (Mg) Bob	Ki trade communication overhead for over head. generate many (ki) 28 bit key: Ki K2-Kn) Mi M2 Mn 64 bit key: Si SzSn 64 bit key: Si SzSn 5 equence #: titztn 5 equence #: titztn Esi (ti, Ki, h(ki))=Mi Esi (ti, Ki, h(ki))=Mi Esi (ti, Kn, h(kn))=Mn (tin, Kn, h(kn))=Mn	randomly pick message mi
trade communication overhead for computation over head. generate many (k) 28 bit key: (k) 64 bit key: (s) 52 Sn (sequence #: t, tztn (sequence #: t, tztn (ti, k), h(k))=M1 Esi (ti, k), h(k))=M2 Esi (ti, k), h(k))=M2 A, I choose to atk Mi (b) (b) (c) (c) (c) (d) (d) (d) (d) (e) (e) (e) (f) (f) (f) (f) (f	A, B (Epub_B) (Msg) A, B (Epub_B) (Signpin (Msg)) Bob	try to establish a key: 128 bit trade communication overhead for over head. generate many (ki) 28 bit key: (ki, kz-kn) 64 bit key: (ki, kz-kn) (ki) 64 bit key: (ki, kz-kn) 65 bit key: (ki, kz-kn) 66 bit key: (ki, kz-kn) 66 bit key: (ki, kz-kn) 67 bit key: (ki, kz-kn) 67 bit key: (ki, kz-kn) 68 bit key: (ki, kz-kn) 68 bit key: (ki, kz-kn) 69 bit key: (ki, kz-kn) 69 bit key: (ki, kz-kn) 60 bit key: (ki, kz-k	randomly pick message mi
trade communication overhead for computation over head. generate many (ki) 28 bit key: K, K2-Kn) 64 bit key: S, S2Sn sequence #: t, t2tn sequence #: t, t2tn Es(t1, K1, h(K1))=M1 Es(t2, k2, h(K2))=M2 Es2(t2, k2, h(K2))=M2 A, I choose ti atk Mi 64 bit ti Kih	A, B (Epub_B) (Signpri_A (Msg)) Bob	Kit trade communication overhead for over head. generate many (ki) 128 bit key: \$1 \$2 \$n 64 bit key: \$1 \$2 \$n sequence #: \$1 \$2 \$t \$equence #: \$1 \$2 \$t \$Esi (\$t1, \$K1, \$h(\$k1))=M1 Esi (\$t2, \$k2, \$h(\$k2))=M2 A. I choose \$t_1^2 Esi (\$t1, \$k1, \$h(\$k1))=Mn The sequence of the sequenc	randomly pick message mi
trade communication overhead for computation over head. generate many (ki) 28 bit key: K, K2-Kn) 64 bit key: S, S2Sn sequence #: t, t2tn sequence #: t, t2tn Es(t1, K1, h(K1))=M1 Es(t2, k2, h(K2))=M2 Es2(t2, k2, h(K2))=M2 A, I choose ti atk Mi 64 bit ti Kih	A, B (Epub_B) [Signpii_A (Mg)] Bob	try to establish a key: 128 bit trade communication overhead for over head. generate many (ki) 28 bit key: (ki, kz-kn) 64 bit key: (ki, kz-kn) (ki) 64 bit key: (ki, kz-kn) 65 bit key: (ki, kz-kn) 64 bit key: (ki, kz-kn) 65 bit key: (ki, kz-kn) 65 bit key: (ki, kz-kn) 66 bit key: (ki, kz-kn) 66 bit key: (ki, kz-kn) 67 bit key:	randomly pick message mi
trade communication overhead for computation over head. generate many (k) 28 bit key: (k) 64 bit key: (s) 52 Sn (sequence #: t) t2 tn (sequence #: t) (t2 tn (t1, K), h(K))=M1 Esi (t1, K), h(K))=M2 Esi (t2, k2, h(K2))=M2 A, I choose ti atk Mi (44 bit (54 b	A, B (Epub_B) [Signpria (mgg)] Bob	trade communication overhead for over head. generate many (ki) 28 bit key: (k, k2-kn) 64 bit key: (s, 52Sn (sequence #: t, tztn Esi (t1, K1, h(k1))=M1 Esi (t2, k2, h(k2))=M2 A whoever	randomly pick message mi
trade communication overhead for computation over head. generate many (k) 28 bit key: (k) 64 bit key: (s) 52 Sn (sequence #: t, tztn (sequence #: t, tztn (t1, K1, h(K1))=M1 Esi (t1, K1, h(K2))=M2 Esi (t2, k2, h(K2))=M2 A, I choose ti atk Mi (64 bit (54 bi	A, B Cpub_B Signpring (mgg)] Bob	try to establish a key: 128 bit trade communication overhead for over head. generate many (ki) 28 bit key: (ki, kz-kn) 64 bit key: (ki, kz-kn) (ki) 64 bit key: (ki, kz-kn) (ki) 64 bit key: (ki, kz-kn) (ki) (ki) (ki) (ki) (ki) (ki) (ki) (ki	randomly pick message mi
trade communication overhead for computation over head. generate many (k) 28 bit key: (k) 64 bit key: (s) 52 Sn (sequence #: t, tztn Sequence #: t, tztn Esi (t1, K1, h(K1))=M1 Esi (t2, k2, h(K2))=M2 Esi (t1, Kn, h(Kn))=Mn Ti (th, Kn, h(Kn))=Mn A whoever	Bob Bob	try to establish a key: 128 bit trade communication overhead for over head. generate many (ki) 28 bit key: (ki, kz-kn) 64 bit key: (ki, kz-kn) (ki) 64 bit key: (ki, kz-kn) 65 bit key: (ki, kz-kn) 64 bit key: (ki, kz-kn) 65 bit key: (ki, kz-kn) 65 bit key: (ki, kz-kn) 66 bit key: (ki, kz-kn) 67 bit key: (ki, kz-k	randomly pick message mi
trade communication overhead for computation over head. generate many (k) 28 bit key: (k) 64 bit key: (s) 52 Sn (sequence #: t) t2 tn (sequence #: t) (t2 tn (t1, K), h(K))=M1 Esi (t1, K), h(K))=M2 Esi (t2, k2, h(K2))=M2 A, I choose ti atk Mi (44 bit (54 b	Bob	trade communication overhead for over head. generate many (ki) 28 bit key: (k, k2-kn) 64 bit key: (s, 52Sn (sequence #: t, tztn Esi (t1, K1, h(k1))=M1 Esi (t2, k2, h(k2))=M2 A whoever	randomly pick message mi
trade communication overhead for computation over head. generate many (k) 28 bit key: (k) 64 bit key: (s) 52 Sn (sequence #: t) t2tn (sequence #: t) (t2tn (t1, K), h(K))=M1 Esi (t1, K), h(K))=M2 Esi (t2, k2, h(K2))=M2 A, I choose ti atk Mi (44 bit (44 bit (47 ki) (47 ki) (47 ki) (48 bit (47 ki) (48 bit	Bob	trade communication overhead for over head. generate many (ki) 28 bit key: (k, k2-kn) 64 bit key: (s, 52Sn (sequence #: t, t2tn Esi (t1, K1, h(k1))=M1 Esi (t2, k2, h(k2))=M2 A whoever	randomly pick message mi
trade communication overhead for computation over head. generate many (k) 28 bit key: (k) 64 bit key: (s) 52 Sn (sequence#: t) (t) (t) (t) (t) (t) (t) (t)		trade communication overhead for over head. generate many (ki) 28 bit key: \$1 \$2 \$n 64 bit key: \$1 \$2 \$n \$equence #: \$1 \$2 \$n \$equence #: \$1 \$1 \$2 \$n \$Esi (\$t1, \$K1, \$n(\$k1)) = M1 Esi (\$t2, \$k2, \$n(\$k2)) = M2 \$Esi (\$t3, \$k3, \$n(\$k2)) = M2 \$Esi (\$t4, \$k1, \$n(\$k2)) = M2 \$Esi (\$t4, \$k1, \$n(\$k2)) = M2 \$Esi (\$t4, \$k2, \$n(randomly pick message mi