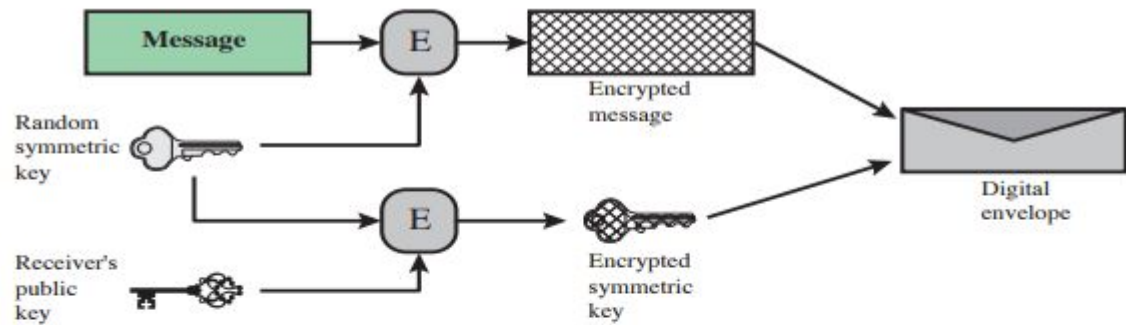


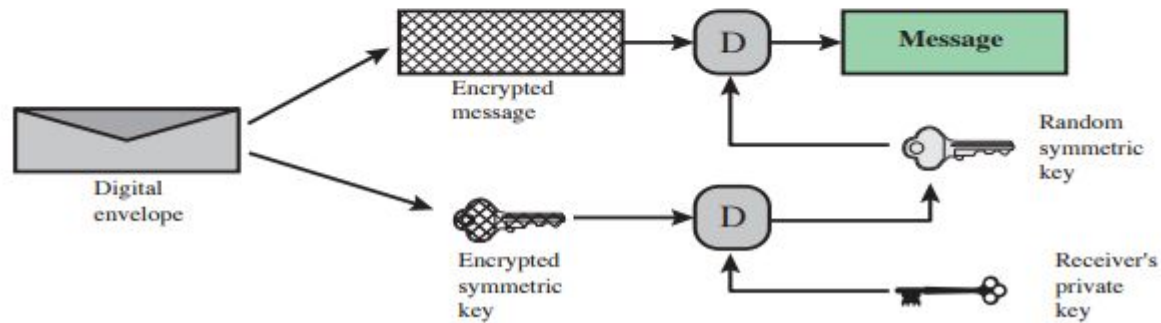
Option 3

...

Chris Brodski



(a) Creation of a digital envelope



(b) Opening a digital envelope

Sender

Sends these byte files::

- Hash number: $H(K_{xy} || M || K_{xy})$
- Encrypted message: $En(M, K_{xy})$
- Encrypted Key: $En(K_{xy}, K_{y+})$

Receiver

Receives:

- Hash number: $H(K_{xy} || M || K_{xy})$
- Encrypted message: $En(M, K_{xy}) = C_M$
- Encrypted Key: $En(K_{xy}, K_{y+}) = C_k$

Decrypts

- $D(C_M, K_{y-}) = M$
- $D(C_k, K_{k-}) = K_{xy}$
- Calculates $H(K_{xy} || M || K_{xy})$ and compares with received hash value.

“Intro_01.pdf” byte file

- I converted the file “Intro_01.pdf” to a byte file (taken from blackboard)
- This is what a text editor sees (next page):

First 50 lines

“Intro_01.pdf” byte file

```

1 %PDF-1.3
2 %Ããöäëó ðÄÊ
3 4 0 obj
4 << /Length 5 0 R /Filter /FlateDecode >>
5 stream
6 xSOPzrYqDCLyîse,Èis SUBEONü=ZuoÜNÜ-uÿÿiaô'2âeGY(iôGeÂCRSeFote)(¥ø:ZlyANUPVTxY=>XêMúF&W
7 ZBf ESSOSOabCSOEd:SWZEt;Y?EsStA8G-šv²y¿Eæ'·ÔeoÖS(µo·ÖÜ'ýp¹kt=VUTÉFijSlôoöyBSjy²ORS>-töå
8 f·s·o'ôä'-EöSIXYZU)s_ð'«i¹«SIO t,uªu-)CAd(c;wE)fwMDDDBEÉYrPBiOS)SORSL°k';£dUmQ'wjÝ.XE:I
9 IIVSgûMizocG(yDCSävES+ig007L·ØY'E;iZ YÝEMEPOTZq;ç(Vn@
10 CACTX,²°CxCTBZÉfj]
11 VñdSYN·dlÖENQ·cÁLá·â+iI,DCCACQIZ3EEdg4BEtoIPñwxÅ#Qñcy;"CPPEvzvž
12 ,FF-iÄAARCKpEdÚráSO·ÜöETINE?U?PaDLlcaapXHÓ!)-u|r"œÑESCRS:SYNALE'Ra+,DCLu,scetDC3|<'CEñATQ°,
13 ~ajöUÖL,j XbÄt3B'VBfr~·ðI}eÉ'E3Ä.UyçTXYÇÄ-?'ÀEEVEFS³=ä-e-cýDDBS/cÄ+9ä,ð
14 [DPS]/V4v---7tSc,SûZhñDDBE-äöSOH/RZYÜCAN/A'-GS")·ÖKBSJ44ú·CAN·é,ŠSYNeE'CB"uÄÖWTÉ-K;|ññE
15 r'DCGPhùe"l)Bx+"bzis_0[ÖTUSQEm]JE6DC33ütDC3'ûSTXCeX·Yè5;OcÅ·vnÖVDEPO"MSORAYææ,ðEäaS"æel
16 NøVDSSV'·CÜÄ="h,WpsRYÄDCC";ç<çCCLMSCöo_R)ñFEÄZLa÷±BEB'ÍbTe:'m'/uik~"bV(Z(SAoZ·SUBIÄ-·ky±
17 *Ü·d·X·CQA·ifIDBSöIN"mINYFN·iC+ENOPeæÜöS5äs"+:xpSYNEFB
18 KEç×fo
19 w8ZÖ+h)ÑÄ-ÖzpöEMV+GES-ßBBNUH+íC'DDB/NAXsäXEM'ECKEZ"ø4-RGaÜACKihl nē.:SUB(NÑœ[SÖ·05'+tEz
20 KËÜ;·'öUKÄ"·Ä SUBESCO-1av'öETNX²·E=s-ÄÆ±:æESCRSç's'dç'yèmFDDCSE[K.KACKEDeSpaÜES-]9AJæYÖÉÉ+'
21 ÖAAæRUFVDTBç<c|:H7föENOCSES.AP)KãoS+*;Ü2EBAACKU
22 GSG2FÄCKA
23 "ZuEPöçeyurrUS!DTEÜÜ-xÑERS·Eep-STXEMCO·Äety kEMr'ò·sESSENQOI'E"<«öbâÄiHZVYH'ARHe'
24 LfeKBpHSYNESCO.VP-Uë+dC&K SOENODCQ'·KÖEMwpÜngCepüdC<2öðAEOTA-ö·ENO;yÖ,Hzi-dpi-Iii[ù+NUM
25 ÜZPökGÜS&ELD·chIKGÄViHYwDC4EEDBöbSYNO5pöAtÄ[AJ,;- -ÖÄ·EKzhJMÍ(Y·ÜE-vä
26 EGOZBEME·BOTil,-GSi)+ikGöi^;EVGE;BSUsySTX,döi
27 endstream
28 endobj
29 5 0 obj
30 2651
31 endobj
32 2 0 obj
33 << /Type /Page /Parent 3 0 R /Resources 6 0 R /Contents 4 0 R /MediaBox [0 0 612 792]
34 >>
35 endobj
36 6 0 obj
37 << /ProcSet [ /PDF /Text ] /ColorSpace << /Cs1 7 0 R /Cs2 8 0 R >> /Font <<
38 /TT11 19 0 R /TT3 11 0 R /TT5 13 0 R /TT7 15 0 R /TT2 10 0 R /TT9 17 0 R >>
39 >>
40 endobj
41 20 0 obj
42 << /Length 21 0 R /N 3 /Alternate /DeviceRGB /Filter /FlateDecode >>
43 stream
44 xSOPUBÖÜTC4?toR=SYN? XG+SÄ US[i ESOSUB-EACK"YiJSYNyé0·$ä:7beSCCBELÜeqO(7ACKüSOHöUEPXSI
45 ACKö(UöÄ IS+*IH(èAS!)&iENOUäwb'SÄIdüE9Bgç;c'ÜD= iusBMU'-«öI9·"§SYN"ZMSÖ·ÖKEPNQ«en-'ÉIDC..
46 rm:NAR·Ö)(öçOutSYN:NPöüE)("QIU·SUBäip+šK+ð+0914[1DC3 BEFDOShu70>Skk?iSöEACK·æIfi'kkttügYç
47 æöäYURÜü+YèÜB+£Ä?è·iö'ADpöpen"- ETBÖB;j,EM;(§*)+ý(')'YLSctY"ý§)'·',ENQ9»itYt0[¬ACDSYS]hv
48 *jMt(-ñEOTCAN;S;EACKACK·ETÄ,atSYNYÜY";R6EXöð$sv·æä-Sx:žš'Hti·OÄCQ3STX·Zhe'æø';ETXöp'DC30:::
49 t>pI[-ACA:SO·IevöEENAKWÜ~") [E,2]Öö+NARi4NARIä(6w,·ÄÄ$%xf"ZèAPöEvYFSmi[D+yä;èVh[ DC3]>

```

“Intro_01.pdf” byte file (top of file)

Observe first few lines

```
1 %PDF-1.3
2 %Āāōāēšó ĐĂĒ
3 4 0 obj
4 << /Length 5 0 R /Filter /FlateDecode >>
5 stream
6 xSOH*ZirYqDCLyise,E!$ SUBEOT;û"Euò&NÜÔ·uUÈYfi&Ó'2ăøGŸ(ióGêÁÇRS EOT@{¥@;žlyANULVTœY=»Xè*úF*W
7 2ĐÍ" ESC SOmbCÓSIêû< STX2C•;Ý?ÈxSIaôG-šv* zÝjèE* ·ò@oŌ$ {µó•ÖÚ"ýµ*ikI=vU7èFijSioŌóýRSjŸ* *ORS>~tôä
```

“Intro_01.pdf” byte file (end)

```
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
12571 0001518887 00000 n
12572 0001528565 00000 n
12573 0001528973 00000 n
12574 0001529242 00000 n
12575 0001538183 00000 n
12576 0001538790 00000 n
12577 0001539052 00000 n
12578 0001551994 00000 n
12579 0001552954 00000 n
12580 0001552359 00000 n
12581 0001552933 00000 n
12582 0001553196 00000 n
12583 0001565852 00000 n
12584 0001566313 00000 n
12585 0001566542 00000 n
12586 0001579489 00000 n
12587 0001580240 00000 n
12588 0001579768 00000 n
12589 0001580219 00000 n
12590 0001580487 00000 n
12591 0001588993 00000 n
12592 0001589745 00000 n
12593 0001589275 00000 n
12594 0001589724 00000 n
12595 0001589995 00000 n
12596 0001599271 00000 n
12597 0001599781 00000 n
12598 0001599460 00000 n
12599 0001599760 00000 n
12600 0001600032 00000 n
12601 0001602843 00000 n
12602 0001603278 00000 n
12603 0001603506 00000 n
12604 0001614459 00000 n
12605 0001614482 00000 n
12606 0001614515 00000 n
12607 0001614569 00000 n
12608 0001614601 00000 n
12609 0001614621 00000 n
12610 0001614651 00000 n
12611 0001614694 00000 n
12612 0001614714 00000 n
12613 trailer
12614 << /Size 308 /Root 253 0 R /Info 1 0 R /ID [ <7fd7025bc08a4189413418ea43a7581c>
12615 <7fd7025bc08a4189413418ea43a7581c> ] >>
12616 startxref
12617 1614922
12618 %%EOF
12619
```


“Intro_01.pdf” byte file (end of file)

```
12609 0001614621 000000 n
12610 0001614651 000000 n
12611 0001614694 000000 n
12612 0001614714 000000 n
12613 trailer
12614 << /Size 308 /Root 253 0 R /Info 1 0 R /ID [ <7fd7025bc08a4189413418ea43a7581c>
12615 <7fd7025bc08a4189413418ea43a7581c> ] >>
12616 startxref
12617 1614922
12618 %%EOF
12619
```

(K || M || K) top of file

- 1234123412341234 = Key

```
1 1234123412341234%PDF-1.3
2 %ÃÀòàë$ó ĎĚ
3 4 0 obj
4 << /Length 5 0 R /Filter /FlateDecode >>
5 stream
6 xSOH%ZirYqDC1ýİse,Ě!$ SUBEOT;û"Eu0&NÜÖ·uÜËýİi&Ó'2ãøGŸ(iÓGêÁÇRS EOT@{¥@;žlyANULVTxÝ=»Xè+úF*
7 2Đí"ESC(SOpbCÓSIêû<STX2E·;Ý?ÈxSlaöG-šv+zÝjèE*·òooô${µó·ŌŰ"ýp*ikT=vU7èFijSioôóýRSjÿ*ORS>~tč
8 f·s÷Ö"òâ\²-ĚóSTXŸZU>s_ð²«i'4<SIO†.p*u-)E4δ[c;wE)fwmDLE DLEEE|ÝrPPÍÖ)SORS1°^k';£ôÜMq'wjÿ...XĚ
9 ĪiVtSgùMizøcG(yDC3ävES+iu007L÷ØY"ě;iZ ýŸEMEOTŽ;Ÿ>{¥n@
10 CBETX,¹°CxETBŽĚfj]
```

(K || M || K) bottom of file

- 1234123412341234 = Key

```
12613 trailer
12614 << /Size 308 /Root 253 0 R /Info 1 0 R /ID [ <7fd7025bc08a4189413418ea43a7581c>
12615 <7fd7025bc08a4189413418ea43a7581c> ] >>
12616 startxref
12617 1614922
12618 %%EOF
12619 1234123412341234
```

message.aescipher

- Message after encryption

```
1  ESC: 0T3eGSfJ-DC45DC3dAe0"SIYyvesBOTZau"OI<A-<l0...c;x"UE*DConLo
2  v+RSERAu6eEA)ER!oé)6B'E-y)DC1r:SYN=AC3a0a0EM-!SOiZ~0"xÉ;â;-6xIa!é#
3  71FB-q$Aî°PyES+e8(0zm)V7h;wâe(ôYéIDC4É.SIks00>?éfi)A0D3âfpqr~-.B+ENOVEN0, fY+-SYNUsd(É°CAN
4  *Gx~mP ÂûAY<"ø) ôi>t'hUS=SUB;0°SYNUq=ô->ÛÂâezOYÊs'NŠjFUS'9xÂÇ.0T3HBB3iâEšwrbbsEBOHÂ00-â×BS
5  "WÊDC30èS1-â+BOT000SOHm...Itegtl: 'œçšNîaueC4~*s:--BSûk
6  SUB0+"qC-ô..DIAfqI
7  Âl&9SO)α(5DC31s=USesBOT0°iRZ
8  Û°âzE3DC3f8fâ;ESCα°?ESCÛæZÛKmlE61ENQixmqôf>="DC3KRSp{DwDC4SO'Â0TNgç=;BS'ôaaNîlîe-ôîû"~Hu
9  SOHEMOIc°hP"z
10 #p°B+m'7(ES00)H'°3°[Ó°Bva+N,0°DC3°uZ+yV7;"iû<EÂ Ûq.ø;LX.ePEUEGS3pSI US°i±êPTXÊESCEDC1)ô0<-
11 âû-°f..i±iESYN4x6j}ÂÛ0Dm[iâê90âææcVPgEÛ w0âtt0).%œfæYôPTXUSNARôér;PTXÊx., B3°SOHPU=, US
12 û&5, /...eNÖL+æzcN4°DC3SUB°;:;wûEi°8°SÂBELvU0z2SUB3°'W4F4°[K.0jE9cç,B*4'wVvcAê(4cêCAN+NUl.œ
13 éÊA>êL: NcDC4!DTEH)kAî #)DC30tiESAbWsp+LZUSNaxC~°DDECAN/p×HgfNUU0CIVak°gic~.-.ÂiACK°SUF
14 YZBpH°Y00QST)æza°G±ûSESC0+-'7q'iîU9STX°-Vp;)NŠ0u&3ETB3aCNUl.°,DšY'Z.ç
15 0YSOHEDE3â:RSdY7Mf+YÊ°UNAYP1°.œ'E~YmâJ0.0°V7uDC3XxER.0T30?ci' N°t<ZÛA)\œSFIâ°~.uPTXkAâ
16 Kâ°aIc&ûN$EÛ -ESC°#iYÂACKEIBi0' Tiu'yÂS°ZGÂ!>èøe
17 V°5ÛSTX-æ0c&SOHEAê-C7iSUB"!×X'<cENQ~>+DC3BOT~N, Z0cšZr°s;ÛNmjš--SOH=DC3°k°wç°GSû0Û°SUBZÂ4c
18 0\îe0+°"°yY0'(PTX0:igCÂââ°'âR rzNUUdUÛtW,œv1ec3AAN°kPQ51°<k-011hBET,zpk3E'u
19 °ê°MFç't°±-ESC(Šjuaû<?BOT0°A°0-8°iV7uEYs0e0ENQZ°7Z2ZURs°'RSi+0XZÇâjç-~j)â#Ej9RS°3uP67B&Yu
20 °0.,Rh(Â-SYNU°7SYN,ESC°é60S°PTXM('Hûe180ES0Zs°°°x1SGH=âUT°a0i°°LêH°60S-0T3AÊEšBDC118uE°6'Îp1
21 DC4Y&lSTX°iêfpg0øq 88Z°-bM9Iâ°æmEOT°ESm'ETB°j0j°HZM-œEM0NêI-°îfâ,Yizç0âe°"ÂnâH°EÛâ+âD
22 2Tp0:(E CAN)J8-x
23 R°,ÂN5-0œ.,é°$H(SOH(SOHDC1)E&YACKDC3°#"â"yû°iVY{.,B°šXtœi ST°iC-û°EMwE30ûE0é0BET.°-î5...yh-fEN0St
24 œV°œ8°ROœ.,Â Šâ+RSNAK10ETXDXDCDC4+DENQ
25 ')DC1SO
26 n1°ToY? )h?w'ôç?S1)0)èE3iut+SOHESNAX/<-°'ENQ°ûZRS°#
27 RS°0;nêDC3çE3ââs0°En-!2m°YÂ6s°âP(^ô+;ÂA
28 64.'$i;5!A0ôûB+ç;-âj+X°SOHA°š±H0âSHMÛâ+NAX3°TB11
29 ACKiDS°US7°V73êf/EOI/DTEÛCAN/w#SO0q5°è°DGeEw°RS°°SOHxY°'â°ENQ°ay°4ACKY°+;â+0dEOTY&STXç
30 ôE,,DC1°YI0E3j0çENQL°m°Yf\0-âZ¥sp$MEOTB0C0HREB1-DEÂX°iDC3SYN°--ô;0's+2n°tVjÂ[EPTX°s°mBETû0
31 WESiÛEMUB!ÂSTXûk0-V7°GS
32 Yet<4Y°E-ÂKBT#(5tPTX°M-4+ESV,±.,
33 V7hIjç9JMW°û080°ÛE CAN°YçhplêIpt ,
34 9û°œX°CANq,dt0a RÛ-E SUBAŽH0BEL0,SOH°Z°ÛS V7°s°g°0°ôY
35 TRSÛ0ôION;û°pE3çSTX°m°ûpI-°SYNû°STX0AÎ°°E35;NBTBS%,æwDTEYFS1êm+fc0c4(BET(âDDC10M)Û,É
36 =tû°î°b8S1°(ETB0BET0°°âpé)iCAN/EBREçWY4-B°cémQ/fé{E5°BSG ACK°êâi±+XC0.ÛÂNUU)Û00BETç-fY0E
37 µ;°Aâ°âwESC0V70°s°E3°¥#8EFTicSTX1°LY=Ê7+ic61.Â(DC3=GS°Pm°ôYÛ[0u
38 ESC(PTXÂUÛ0û0P¥CAN/ç9eB°-°DC1+JDP°¥0YéV70ESÂ0°NAX.,iU08e-SYN;BET°yç;ç°Q092pN1<è+œKlÂ°D6
39 âC7VY°XÂPÊS1°e°'Ûc0EAKI°L&,U0EOT
40 fHPDC3i/,Ba! ,PAC3
41 ŽESON°--1c+mNUJDC318vS1B°>DC3x0û,ào?6ÛRSBET~Yçs1USi°'âCAN°âEiDûhg°BOTEMi%,ž #À0fw=ôE°6Û~ynUS
42 m
43 SUB3u°DTEZÂP°gYV7W°âÂ0PC>â°\0sKRA-szx0!±+cXACKYÂ°r°0DC3âi0ç°P.,pocDC33ç-DTE3pU0âApli°O ZRS
44 °°d7-šACK+âB0ÂçIRS6S0g°xi°šIj.,uV7iêBOT0C0hceC'è0cSUBK1°SUB7A°i°i)cS3â°iê°;ÂUš
45 ùP0°+0r3ç°E°\±cMÛ°âH°MNAK°Nâ0ae GZwCAN°SO{...cDm.xG°ç°Q0ô08û°+BETt0é+°ETBYEXFS,DC3°ZPu5iDC4ç
46 7SYNHfHû°DC4DB0jGSVÊE°çQçC°3ââ/°°éœN,ETBŠA-fES0-0SYNÊ°%/ES0SYN°USmp°èâS0°~E?b21NUUûçPTX
47 BEM°..y6âSOiS°=W(1°âçES0âSTX°œEUSBS°0âSYNîi0Y°â0DTEG°SOHIGNUÛSCGZ°-0a# mJ9E;œeNixE°R0B1
48 °v0YÂœ,|BS°ENQ°)°×=EVSYNvecÊ-GDC3B è0v-â0âA°#8°[SYN°0ÊE0âîNgk-0j)œ!cESU°Qâ,°=°Qxû-1p°S1NAX
49 ->GSfyRw°.9xSé°SOalk°ACKYçj):/;ÂYé iD°°ESC°šâi;Aî 0oU°xpESCA+LFAEBÛU00cV70-JDC1ETBAC
```

