

Decryption

Encryption

S-AES

cipher

S-AES

reversecipher

**APPENDIXP**

*SimpliﬁedAES(S-AES)*

**SimpliﬁedAES(S-AES),developed**byProfessorEdwardSchaeferofSantaClaraUniver-sity,isaneducationaltooldesignedtohelpstudentslearnthestructureofAESusingsmallerblocksandkeys.ReadersmaychoosetostudythisappendixbeforereadingChapter7.

**P.1S-AESSTRUCTURE**

S-AESisablockcipher,asshowninFigureP.1.

**FigureP.1*Encryption****anddecryptionwithS-AES*

16-bitplaintext

16-bitplaintext

16-bitkey

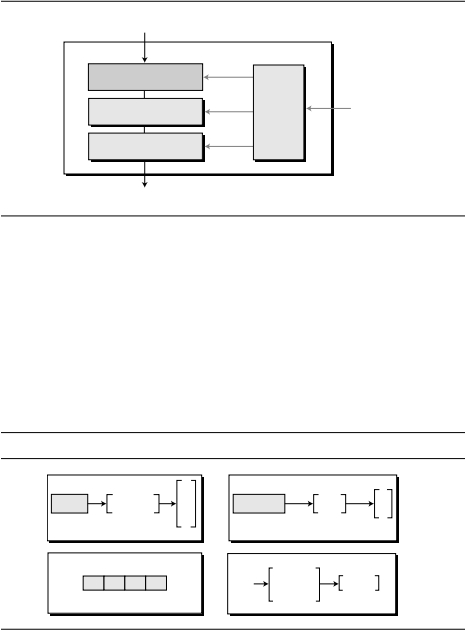
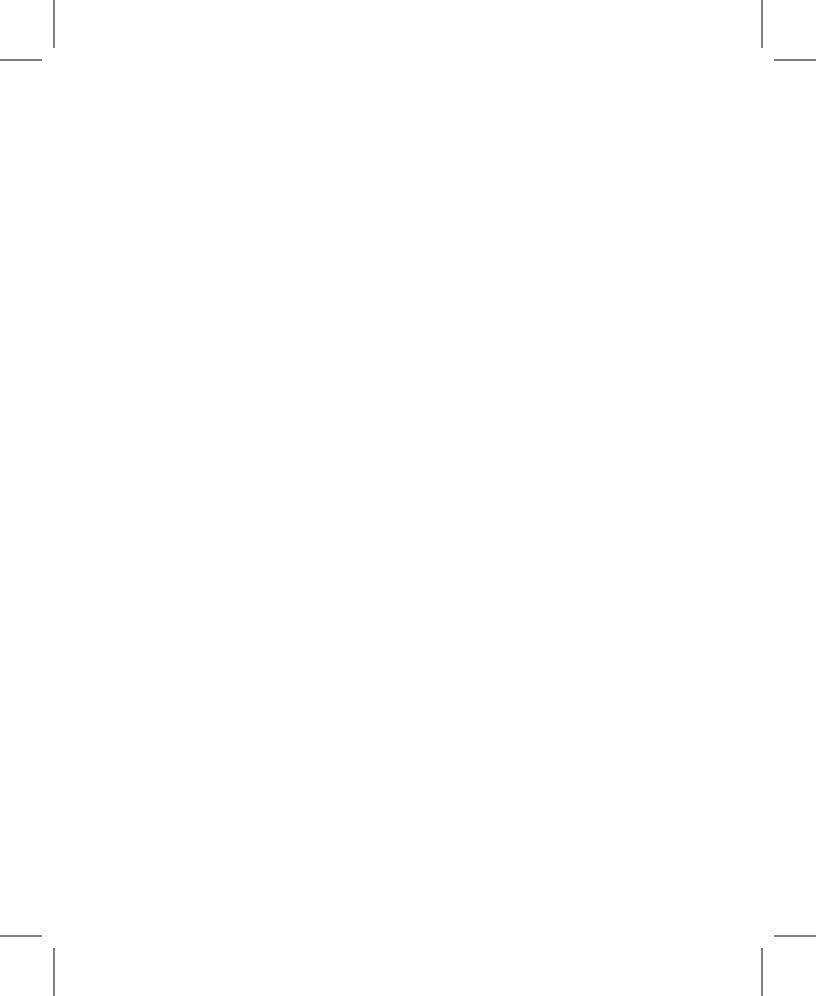
16-bitciphertext

16-bitciphertext

Attheencryptionsite,S-AEStakesa16-bitplaintextandcreatesa16-bitcipher-text;atthedecryptionsite,S-AEStakesa16-bitciphertextandcreatesa16-bitplaintext.Thesame16-bitcipherkeyisusedforbothencryptionanddecryption.

1. **ounds**
2. -AESisanon-Feistelcipherthatencryptsanddecryptsadatablockof16bits.Itusesonepre-roundtransformationandtworounds.Thecipherkeyisalso16bits.FigureP.2

**667**



**n**

**1**

**n**

**2**

**n**

**3**

**n**

Nibble

Word

**0**

Round1

**1**

**s**

**s**

**1**

**0**

**0**

2

0

1

Key

expansion

Round2

Pre-round

transformation

b

b

b

b

**n**

bbbb

**n**

Nibble

**n**

3

2

1

0

0123

Block

**668*APPENDIX****PSIMPLIFIEDAES(S-AES)*

**FigureP.2*General****designofS-AESencryptioncipher*

16-bitplaintext

RoundKeys

(16bits)

S-AES

K

0

K

Cipherkey

(16bits)

16-bitciphertext

K

2

showsthegeneraldesignfortheencryptionalgorithm(calledthecipher);thedecryp-tionalgorithm(calledtheinversecipher)issimilar,buttheroundkeysareappliedinthereverseorder.

InFigureP.2,theroundkeys,whicharecreatedbythekey-expansionalgorithm,arealways16bits,thesamesizeastheplaintextorciphertextblock.InS-AES,there

arethreeroundkeys,K

,K

1

,andK

.

**DataUnits**

S-AESusesﬁveunitsofmeasurementtorefertodata:bits,nibbles,words,blocks,andstates,asshowninFigureP.3.

**FigureP.3*Data****unitsusedinS-AES*

Word

**nn**

**ww**

**1**

**n**

**n**

**w**

State

**S**

**s**

**s**

**0,0**

**1,0**

**0,1**

**1,1**

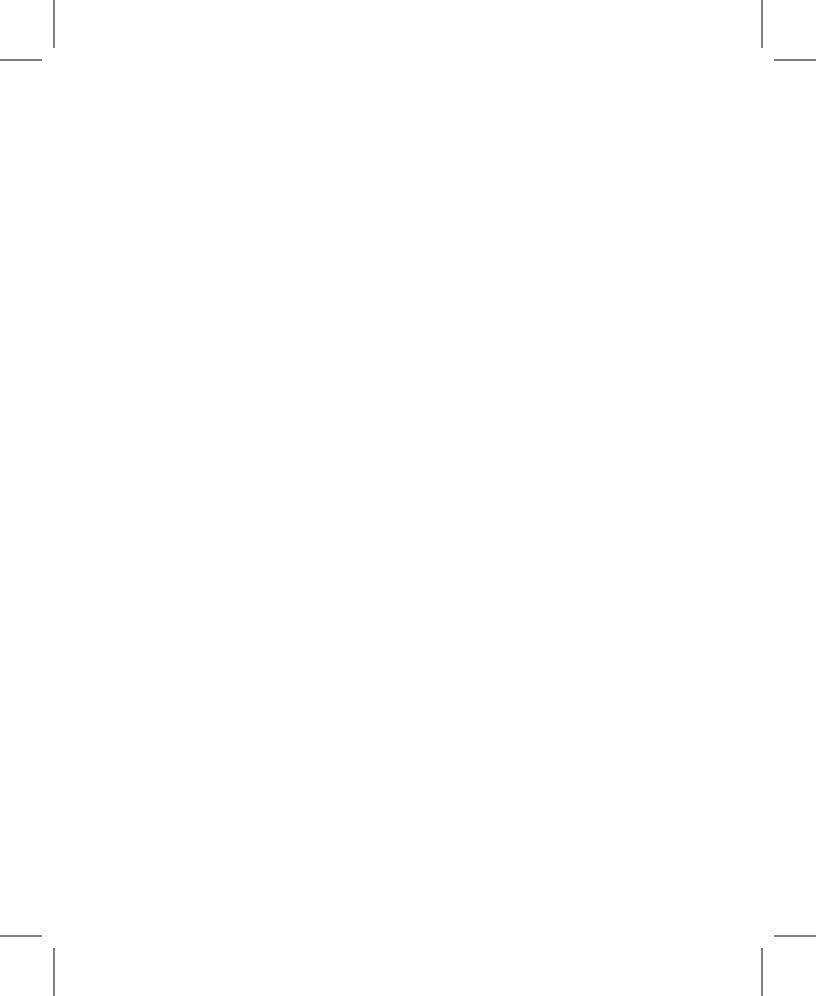
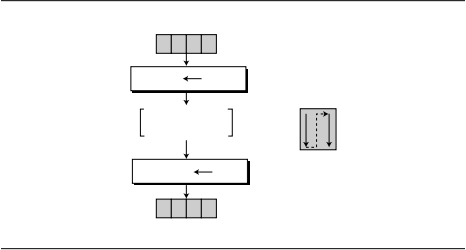
**w**

**0**

**w**

***Bit***

InS-AES,a*bitis*abinarydigitwithavalueof0or1.Weusealowercaseletterbtorefertoabit.



**block**

r+2c

**s**

r,c

**s**

i

imod2,i/2

**block**

**n**

**0**

**0123**

**s**

**s**

**s**

**s**

**123**

*SECTIONP.1S-AESSTRUCTURE****669***

***Nibble***

A**nibbleis**agroupof4bitsthatcanbetreatedasasingleentity,arowmatrixof4bits,oracolumnmatrixof4bits.Whentreatedasarowmatrix,thebitsareinsertedintothematrixfromlefttoright;whentreatedasacolumnmatrix,thebitsareinsertedintothematrixfromtoptobottom.Weusealowercaseboldletter**nto**refertoanibble.Notethatanibbleisactuallyasinglehexadecimaldigit.

***Word***

1. *wordis*agroupof8bitsthatcanbetreatedasasingleentity,arowmatrixoftwonibbles,oracolumnmatrixof2nibbles.Whenitistreatedasarowmatrix,thenibblesareinsertedintothematrixfromlefttoright;whenitisconsideredasacolumnmatrix,thenibblesareinsertedintothematrixfromtoptobottom.Weusethelowercaseboldletter**wto**refertoaword.
2. ***lock***

S-AESencryptsanddecryptsdatablocks.A*blockin*S-AESisagroupof16bits.How-ever,ablockcanberepresentedasarowmatrixof4nibbles.

***State***

InS-AES,adatablockisalsoreferredtoasa*state*.Weuseanuppercaseboldletter**Sto**refertoastate.States,likeblocks,aremadeof16bits,butnormallytheyaretreated

asmatricesof4nibbles.Inthiscase,eachelementofastateisreferredtoas**s**

*r*,*c*

,where

*r(0*to1)deﬁnestherowandthe*c(0*to1)deﬁnesthecolumn.Atthebeginningofthecipher,nibblesinadatablockareinsertedintoastatecolumnbycolumn,andineachcolumn,fromtoptobottom.Attheendofthecipher,nibblesinthestateareextractedinthesameway,asshowninFigureP.4.

**FigureP.4*Block-to-state****andstate-to-blocktransformation*

Block

**nnnn**

State

**0,0**

**1,0**

=**n**

=**n**

**0**

**1**

**0,1**

**1,1**

=**n2**

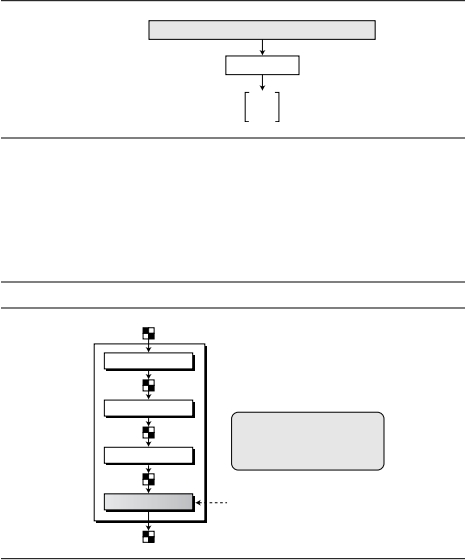
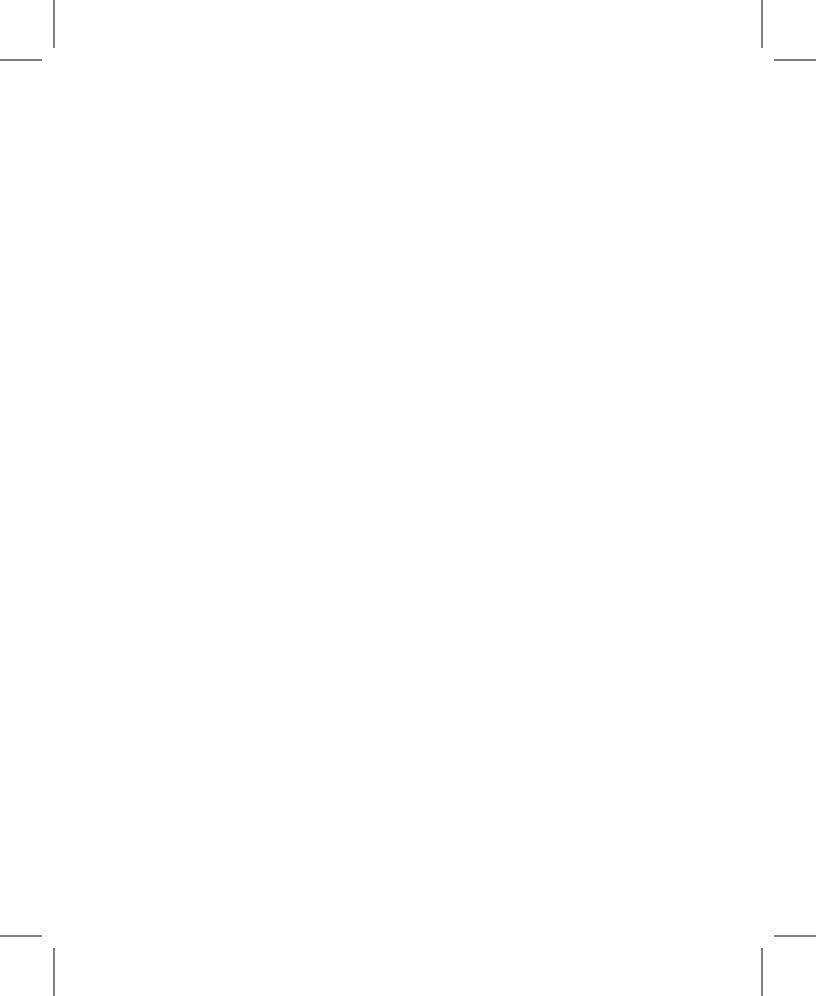
=**n3**

Insertionand

extractionflow

**nnn**

Block



AddRoundKey

MixColumns

**9**

**9**

**6**

**B**

**7**

Block(bits)**1011**

Block(nibbles)

State

**0110**

**1001**

**0111**

**6**

**7**

**B**

Round

State

State

State

1. OneAddRoundKeyisappliedbeforeround1.
2. Thethirdtransformationismissinginround2.

SubNibbles

ShiftRows

**670*APPENDIX****PSIMPLIFIEDAES(S-AES)*

***ExampleP.1***

Letusseehowa16-bitblockcanbeshownasa2×2matrix.Assumethatthetextblockis1011011110010110.Weﬁrstshowtheblockas4nibbles.Thestatematrixisthenﬁlledup,columnbycolumn,asshowninFigureP.5.

**FigureP.5*Changing****ciphertexttoastate*

**StructureofEachRound**

FigureP.6showsthateachtransformationtakesastateandcreatesanotherstatetobeusedforthenexttransformationorthenextround.Thepre-roundsectionusesonlyonetransformation(AddRoundKey);thelastroundusesonlythreetransformations,(MixColumnstransformationismissing).

**FigureP.6*Structure****ofeachroundattheencryptionsite*

State

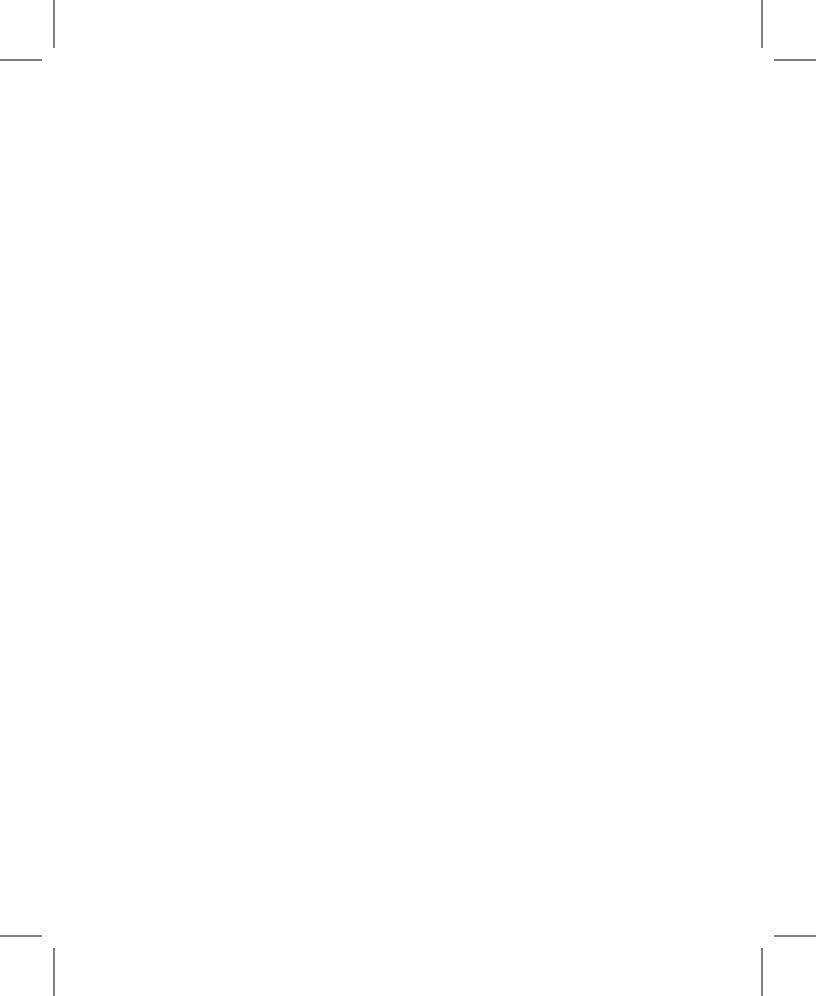
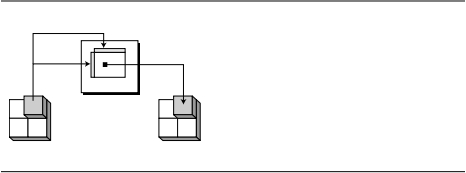
Notes:

Round

Key

State

Atthedecryptionsite,theinversetransformationsareused:InvSubNibbles,Inv-ShiftRows,InvMixColumns,andAddRoundKey(thisoneisself-invertible).



Table

10

32

10

10

16

16

16

16

|  |  |
| --- | --- |
|  | *00011011* |
| *00*  *01*  *10*  *11* | 94AB  D185  6203  CEF7 |

|  |  |
| --- | --- |
|  | *00011011* |
| *00*  *01*  *10*  *11* | A59B  178F  6023  C4DE |

*SECTIONP.2TRANSFORMATIONS****671***

**P.2TRANSFORMATIONS**

Toprovidesecurity,S-AESusesfourtypesoftransformations:substitution,permuta-tion,mixing,andkey-adding.Wewilldiscusseachhere.

**Substitution**

Substitutionisdoneforeachnibble(4-bitdataunit).Onlyonetableisusedfortrans-formationsofeverynibble,whichmeansthatiftwonibblesarethesame,thetransfor-mationisalsothesame.Inthisappendix,transformationisdeﬁnedbyatablelookupprocess.

1. ***ubNibbles***
2. heﬁrsttransformation,**SubNibbles,is**usedattheencryptionsite.Tosubstituteanib-ble,weinterpretthenibbleas4bits.Theleft2bitsdeﬁnetherowandtheright2bitsdeﬁnethecolumnofthesubstitutiontable.Thehexadecimaldigitatthejunctionoftherowandthecolumnisthenewnibble.FigureP.7showstheidea.

**FigureP.7*SubNibbles****transformations*

*aa*

*aa*

*b*

*aa*

*aa*

*a*

SubNibbles

*a*

3

*a*

2

*a*

3

*a*

2

State

State

SubNibblestable

InvSubNibblestable

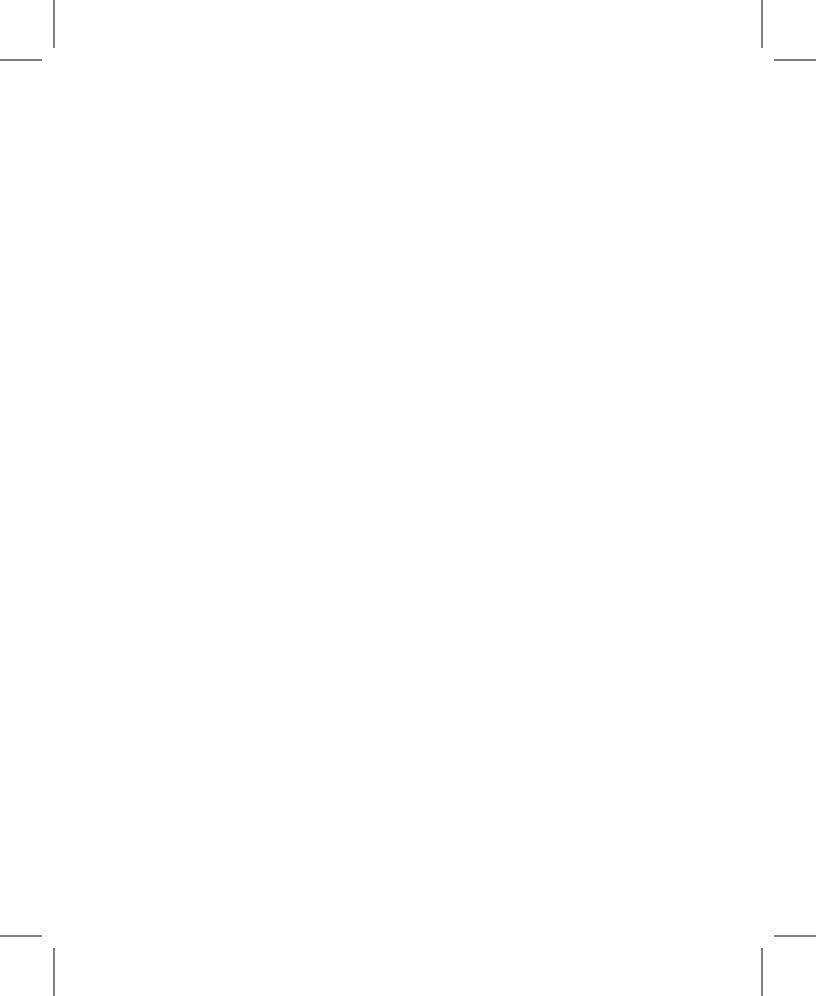
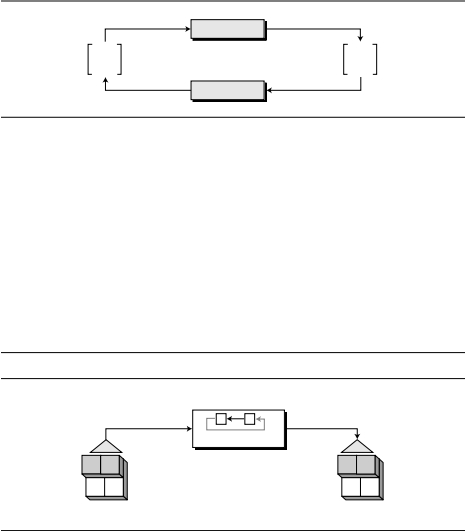
IntheSubNibblestransformation,thestateistreatedasa2×2matrixofnibbles.Transformationisdoneonenibbleatatime.Thecontentsofeachnibbleischanged,butthearrangementofthenibblesinthematrixremainsthesame.Intheprocess,eachnibbleistransformedindependently:Therearefourdistinctnibble-to-nibbletransformations.

**SubNibblesinvolvesfourindependentnibble-to-nibbletransformations.**

FigureP.7alsoshowsthesubstitutiontable(S-box)fortheSubNibblestransforma-tion.Thetransformationdeﬁnitelyprovidesconfusioneffect.Forexample,twonibbles,

AandB,whichdifferonlyinonebit(therightmostbit),aretransformedto03,whichdifferintwobits.

and



Shiftleft

SubNibbles

InvSubNibbles

**State**

**0**

**4**

**9**

**D**

**State**

**672*APPENDIX****PSIMPLIFIEDAES(S-AES)*

***InvSubNibbles***

**InvSubNibblesis**theinverseofSubNibbles.TheinversetransformationisalsoshowninFigureP.7.Wecaneasilycheckthatthetwotransformationsareinversesofeachother.

1. ***xampleP.2***
2. igureP.8showshowastateistransformedusingtheSubNibblestransformation.TheﬁgurealsoshowsthattheInvSubNibblestransformationcreatestheoriginalstate.Notethatifthetwonib-bleshavethesamevalues,theirtransformationarealsothesame.Thereasonisthateverynibbleusesthesametable.

**FigureP.8*SubNibble****transformationforExampleP.2*

**Permutation**

Anothertransformationfoundinaroundisshifting,whichpermutesthenibbles.Shift-ingtransformationinS-AESisdoneatthenibblelevel;theorderofthebitsinthenib-bleisnotchanged.

***ShiftRows***

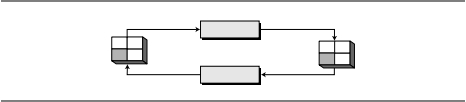
Intheencryption,thetransformationiscalled*ShiftRowsand*theshiftingistotheleft.Thenumberofshiftsdependsontherownumber(0,1)ofthestatematrix.Thismeansrow0isnotshiftedatallandrow1isshifted1nibble.FigureP.9showstheshiftingtransformation.NotethattheShiftRowstransformationoperatesonerowatatime.

**FigureP.9*ShiftRows****transformation*

ShiftRow

Row0:noshift

1. ow1:1-nibbleshift
2. tateState



**C**

**F**

**2**

**6**

InvShiftRows

ShiftRows

**State**

**6C**

**F2**

**State**

*SECTIONP.2TRANSFORMATIONS****673***

***InvShiftRows***

Inthedecryption,thetransformationiscalled*InvShiftRowsand*theshiftingistotheright.Thenumberofshiftsisthesameasthenumberoftherow(0,1)inthestatematrix.

**TheShiftRowsandInvShiftRowstransformationsareinversesofeachother.*ExampleP.3***

FigureP.10showshowastateistransformedusingShiftRows.TheﬁgurealsoshowsthattheInvShiftRowstransformationcreatestheoriginalstate.

**FigureP.10*ShiftRows****transformationinExampleP.3*

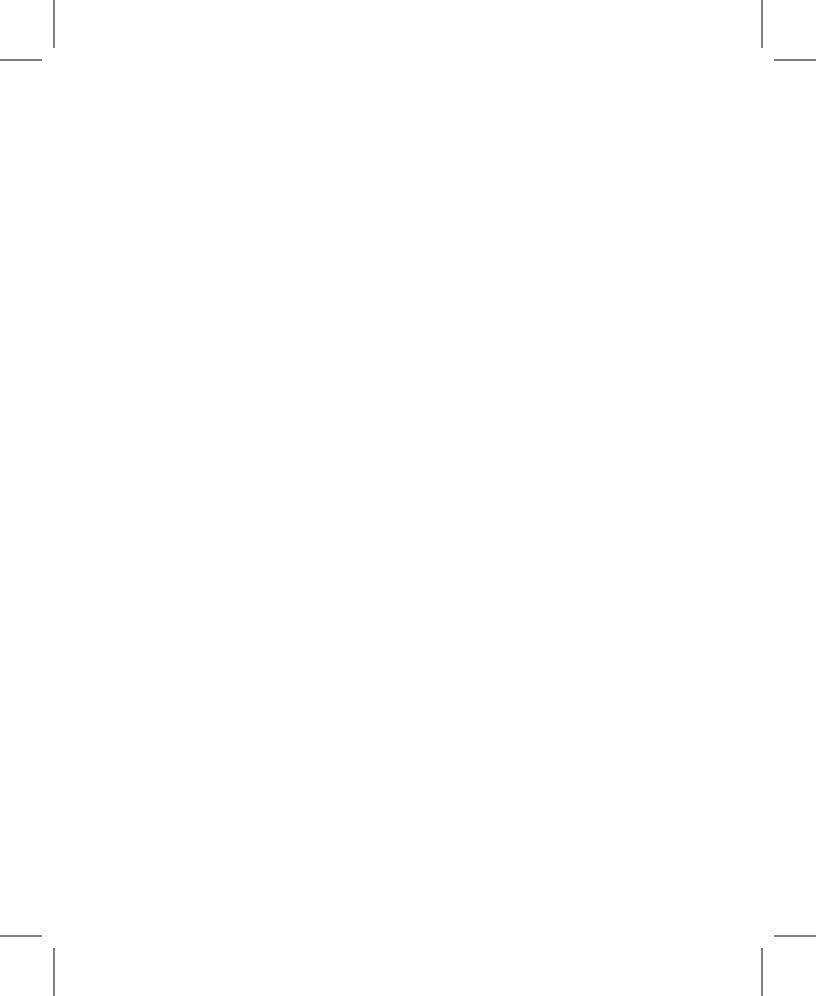
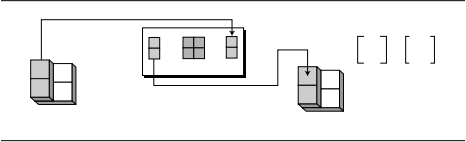
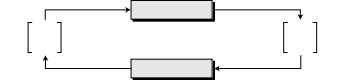
**Mixing**

ThesubstitutionprovidedbytheSubNibblestransformationchangesthevalueofthenibblebasedonlyonthenibble’soriginalvalueandanentryinthetable;theprocessdoesnotincludetheneighboringnibbles.WecansaythatSubNibblesisan*intra-nibbletransformation.*ThepermutationprovidedbytheShiftRowstransformationexchangesnibbleswithoutpermutingthebitsinsidethebytes.WecansaythatShiftRowsisa*nibble-exchangetransformation.*Wealsoneedan*inter-nibbletransformation*thatchangesthebitsinsideanibble,basedonthebitsinsidetheneighboringnibbles.Weneedtomixnibblestoprovidediffusionatthebitlevel.

Themixingtransformationchangesthecontentsofeachnibblebytaking2nibblesatatimeandcombiningthemtocreate2newnibbles.Toguaranteethateachnewnib-bleisdifferent(eveniftheoldnibblesarethesame),thecombinationprocessﬁrstmul-tiplieseachnibblewithadifferentconstantandthenmixesthem.Themixingcanbeprovidedbymatrixmultiplication.AswediscussedinChapter2,whenwemultiplyasquarematrixbyacolumnmatrix,theresultisanewcolumnmatrix.Eachelementinthenewmatrixdependsonthetwoelementsoftheoldmatrixaftertheyaremultipliedbyrowvaluesintheconstantmatrix.

***MixColumns***

The*MixColumnstransformation*operatesatthecolumnlevel;ittransformseachcol-umnofthestateintoanewcolumn.Thetransformationisactuallythematrixmultipli-cationofastatecolumnbyaconstantsquarematrix.Thenibblesinthestatecolumnandconstantsmatrixareinterpretedas4-bitwords(orpolynomials)withcoefﬁcientsin



MixColumns

InvMixColumns

**State**

**6**

**F**

**C**

**F**

**F**

**4**

**5**

**A**

**State**

=

×

Constant

44

**674*APPENDIX****PSIMPLIFIEDAES(S-AES)*

GF(2).MultiplicationofbytesisdoneinGF(2)withmodulus(*x+x+*1)or(10011).AdditionisthesameasXORingof4-bitwords.FigureP.11showstheMixColumnstransformation.

**FigureP.11*MixColumns****transformation*

MixColumns

14

41

92

29

CC

–1

State

State

***InvMixColumns***

The*InvMixColumnstransformation*isbasicallythesameastheMixColumnstransfor-mation.Ifthetwoconstantmatricesareinversesofeachother,itiseasytoprovethatthetwotransformationsareinversesofeachother.

**TheMixColumnsandInvMixColumnstransformationsareinversesofeachother.**

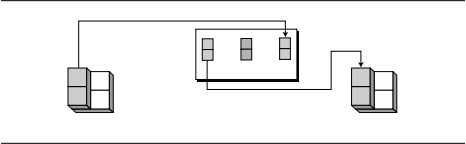
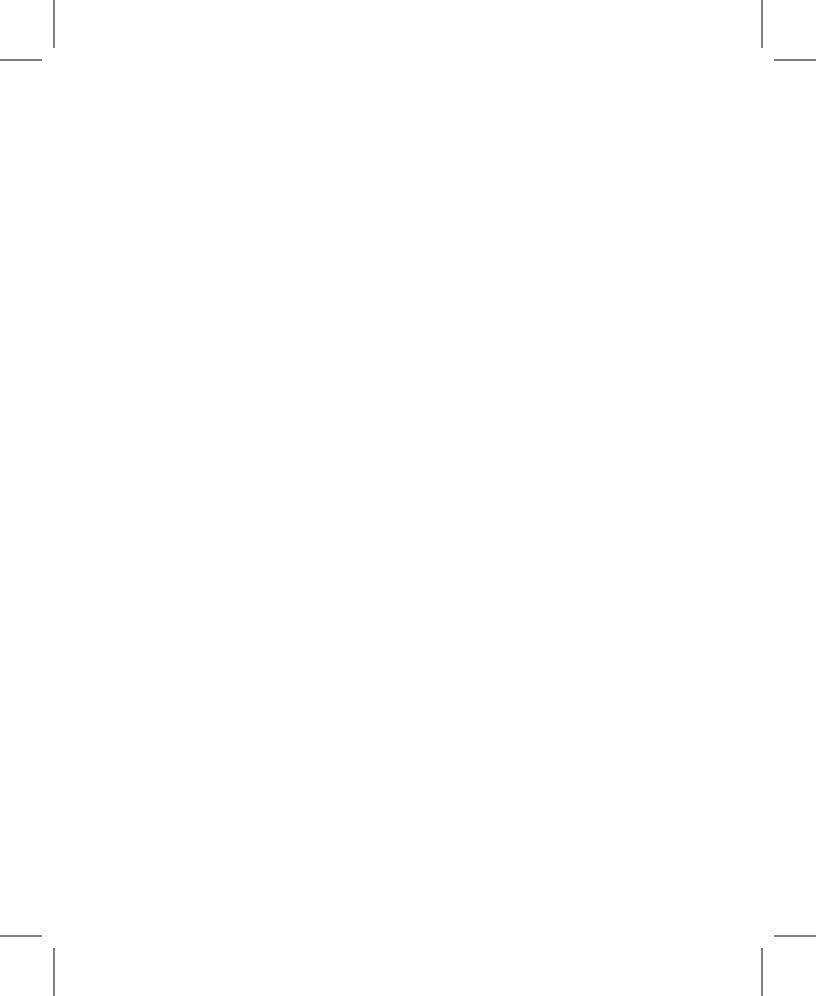
FigureP.12showshowastateistransformedusingtheMixColumnstransformation.TheﬁgurealsoshowsthattheInvMixColumnstransformationcreatestheoriginalone.

**FigureP.12*The****MixColumnstransformationinExample7.5*

Notethatequalbytesintheoldstate,arenotequalanymoreinthenewstate.Forexample,thetwobytesFinthesecondrowarechangedto4andA.

**KeyAdding**

Probablythemostimportanttransformationistheonethatincludesthecipherkey.Allprevioustransformationsuseknownalgorithmsthatareinvertible.Ifthecipher



4

*SECTIONP.3KEYEXPANSION****675***

keyisnotaddedtothestateateachround,itisveryeasyfortheadversarytoﬁndtheplaintext,giventheciphertext.ThecipherkeyistheonlysecretbetweenAliceandBobinthiscase.

S-AESusesaprocesscalledkeyexpansion(discussedlaterinthisappendix)thatcreatesthreeroundkeysfromthecipherkey.Eachroundkeyis16bitslongitistreatedastwo8-bitwords.Forthepurposeofaddingthekeytothestate,eachwordisconsideredasacolumnmatrix.

***AddRoundKey***

*AddRoundKeyalso*proceedsonecolumnatatime.ItissimilartoMixColumnsinthisrespect.MixColumnsmultipliesaconstantsquarematrixbyeachstatecolumn;AddRoundKeyaddsaroundkeywordwitheachstatecolumnmatrix.TheoperationsinMixColumnsarematrixmultiplication;theoperationsinAddRoundKeyarematrixaddition.TheadditionisperformedintheGF(2)ﬁeld.Becauseadditionandsubtrac-tioninthisﬁeldarethesame,theAddRoundKeytransformationistheinverseofitself.FigureP.13showstheAddRoundKeytransformation.

**TheAddRoundKeytransformationistheinverseofitself.**

**FigureP.13*AddRoundKey****transformation*

AddRoundKey

=

+

Keyword

StateState

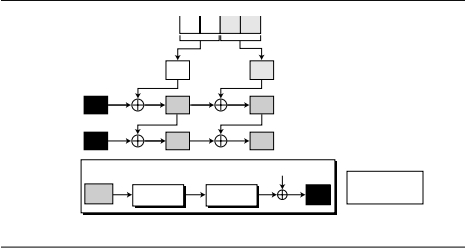
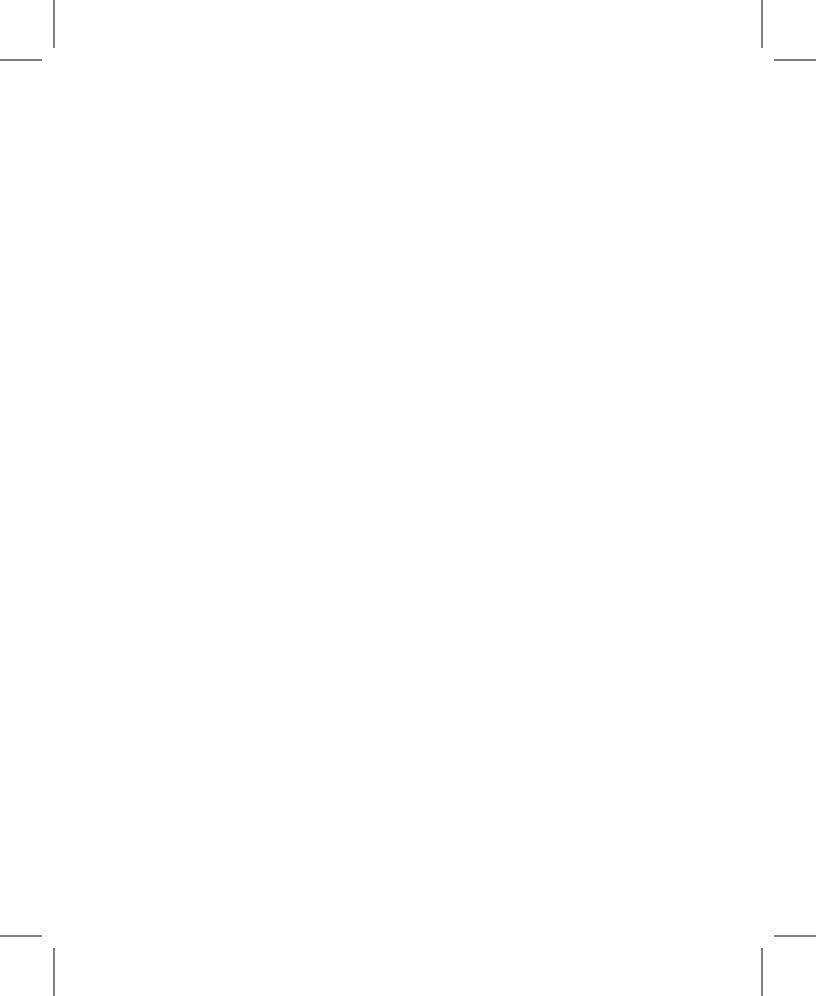
**P.3KEYEXPANSION**

The*keyexpansionroutine*createsthree16-bitroundkeysfromonesingle16-bitcipherkey.Theﬁrstroundkeyisusedforpre-roundtransformation(AddRoundKey);theremainingroundkeysareusedforthelasttransformation(AddRoundKey)attheendofround1andround2.

Thekey-expansionroutinecreatesroundkeyswordbyword,whereawordisanarrayof2nibbles.Theroutinecreates6words,whicharecalled**w**0,**w**1,**w**2,…,**w**5.

**CreationofWordsinS-AES**

FigureP.14showshow6wordsaremadefromtheoriginalkey.



***i***

**n**

3

**n**

2

**SubWord**

**RotWord**

W

*i*−1

16

16

**t**

5

**w**

**w**

4

3

**w**

**w**

2

RCon**[**1**]=**80RCon**[**2**]=**30

*i*

0

3

0

1

0

2

3

1

1

*i*−1

*r*

*r*

24

3

5

**RCon[*Nr*]**

1

**w**

**w**

0

**t**

**2**

**t**

**4**

*i*

**t**

=SubWord(RotWord(**w***i*−1))⊕RCon[*Nr*]

01

***i***

0

**676*APPENDIX****PSIMPLIFIEDAES(S-AES)*

**FigureP.14*Creation****ofwordsinS-AES*

**Cipherkey**

Pre-round

**nn**

Round1

Round2

**Makingoft**

**(temporary)words*i=*2*Nr***

**,where*N***

***r***

**istheroundnumber**

Theprocessisasfollows:

1.Theﬁrsttwowords(**w,w)**aremadefromthecipherkey.Thecipherkeyisthoughtofasanarrayof4nibbles(**nton).**Theﬁrst2nibbles(**nton)**become**w;**thenext2nibbles(**nton)**become**w.**Inotherwords,theconcate-nationofthewordsinthisgroupreplicatesthecipherkey.

2.Therestofthewords(**w**

for*i=*2to5)aremadeasfollows:

a.If(*imod*2)=0,**w***i=***t***i⊕***w***i*−2.Here**t***i*,atemporaryword,istheresultofapply-ingtworoutines,SubWordandRotWord,on**wand**XORingtheresultwitharoundconstant,RC[*N],*where*Nis*theroundnumber.Inotherwords,wehave

Thewords**wandware**madeusingthisprocess.

b.If(*imod*2)≠0,**w***i=***w***i*−1

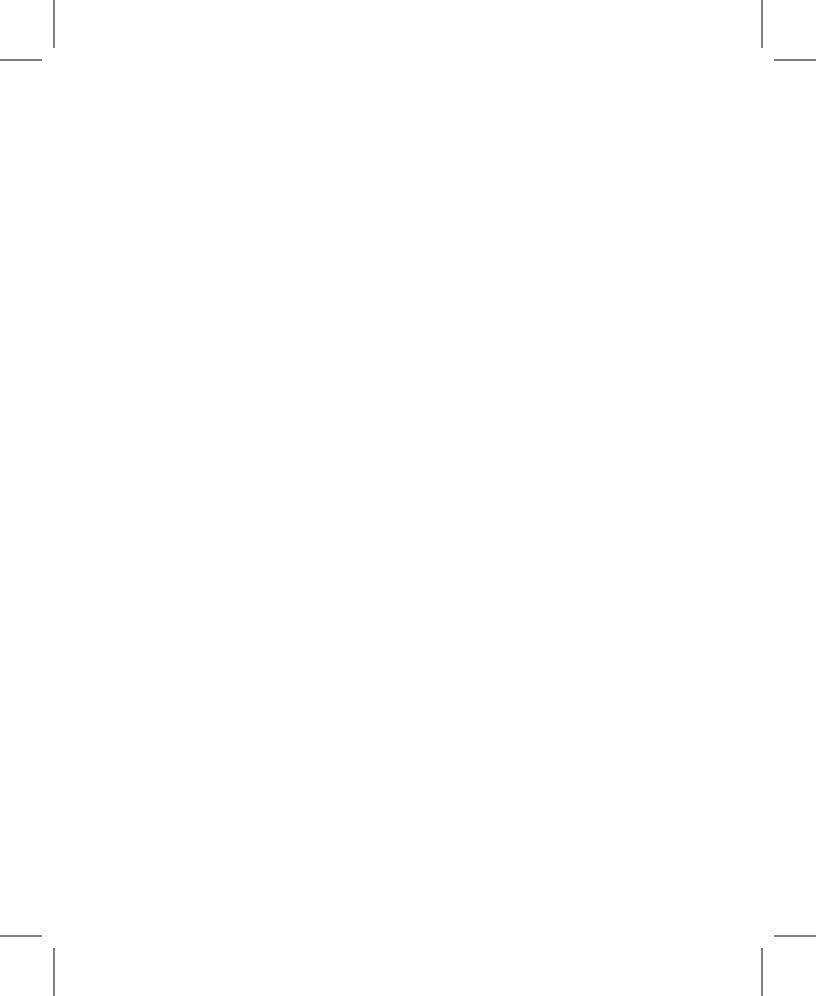
⊕**w***i*−2.ReferringtoFigureP.14,thismeanseach

wordismadefromthewordattheleftandthewordatthetop.Thewords**wandware**madeusingthisprocess.

***RotWord***

The*RotWord(rotate*word)routineissimilartotheShiftRowstransformation,butitisappliedtoonlyonerow.Theroutinetakesawordasanarrayof2nibblesandshiftseachnibbletotheleftwithwrapping.InS-AES,thisisactuallyswappingthe2nibblesintheword.

1. ***ubWord***
2. he*SubWord(substitute*word)routineissimilartotheSubNibbletransformation,butitisappliedonlyto2nibbles.TheroutinetakeseachnibbleinthewordandsubstitutesanothernibbleforitusingtheSubNibbletableinFigureP.7.



**4**

**2**

***i***

**2**

**5**

**4**

**4**

**0**

**3**

**2**

**0**

**1**

**0**

16

**RotWord(75)**=57

**2**

**RotWord(C4)**=4C

*SECTIONP.4CIPHERS****677***

***RoundConstants***

Eachroundconstant,RC,isa2-nibblevalueinwhichtherightmostnibbleisalwayszero.FigureP.14alsoshowsthevalueofRCs.

***ExampleP.4***

TableP.1showshowthekeysforeachroundarecalculatedassumingthatthe16-bitcipherkeyagreeduponbyAliceandBobis2475.

**TableP.1*Key****expansionexample*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***Round*** | ***Valuesof***  ***t’s*** | ***Firstword***  ***intheround*** | ***Secondword***  ***intheround*** | ***RoundKey*** |
| ***0*** |  | **w=24** | **w=75** | **K=2475** |
| ***1*** | **t=95** | **w**  **=95⊕24=B1** | **w**  **=B1⊕75=C4** | **K=B1C4** |
| ***2*** | **t=EC** | **w**  **=B1⊕EC=5D** | **w**  **=5D⊕C4=99** | **K=5D99** |

Ineachround,thecalculationofthesecondwordisverysimple.Forthecalculationoftheﬁrstwordweneedtoﬁrstcalculatethevalueofthetemporaryword(**t),**asshownbelow:

→**SubWord(57)**=15

→**t=**15⊕**RC[1]=**15⊕80=95

→**SubWord(4C)**=DC

→**t**

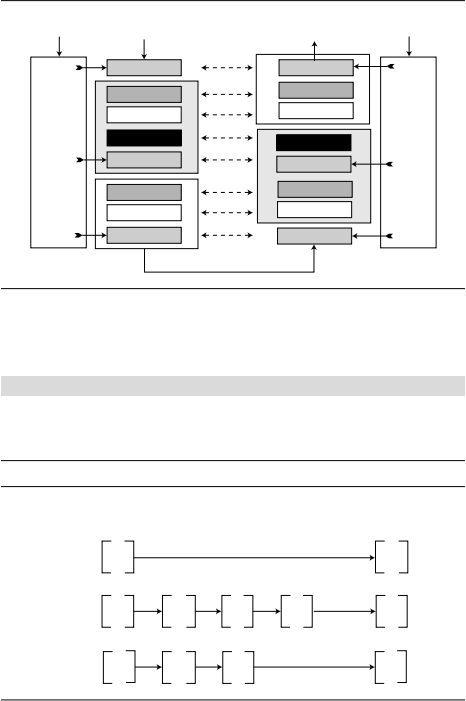
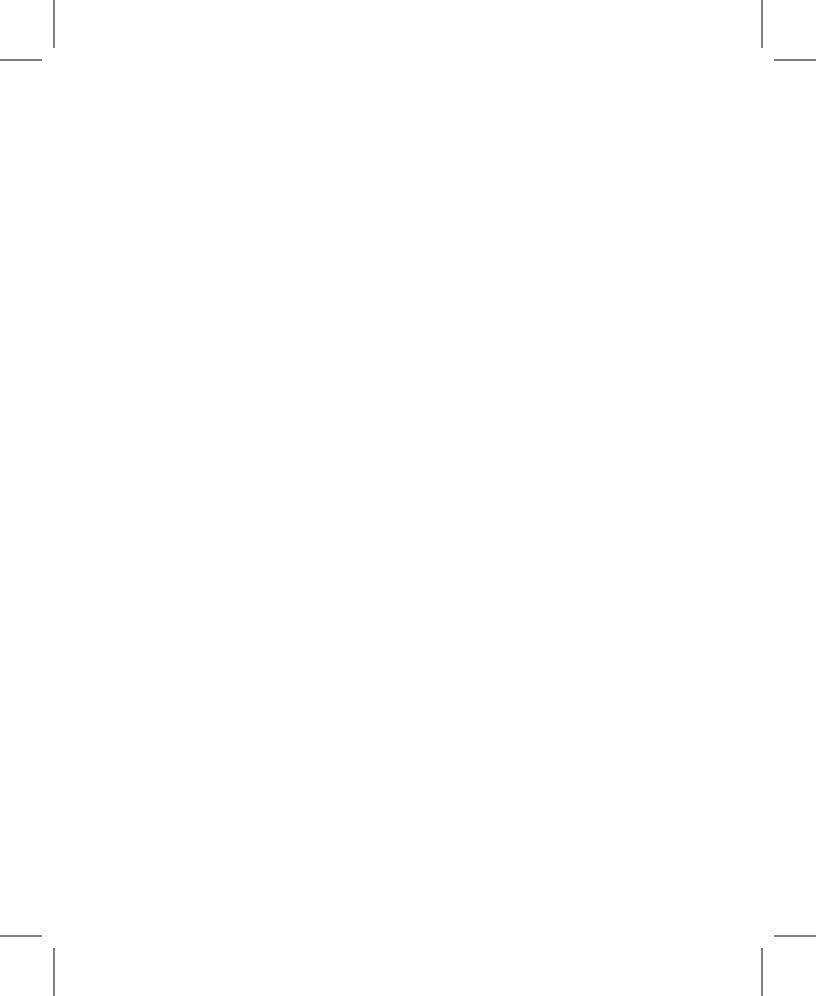
=DC⊕**RC[2]=**DC⊕30=EC

**P.4CIPHERS**

NowletusseehowS-AESusesthefourtypesoftransformationsforencryptionanddecryption.Theencryptionalgorithmisreferredtoasthe*cipherand*thedecryptionalgorithmasthe*inversecipher*.

S-AESisanon-Feistelcipher,whichmeansthateachtransformationorgroupoftransformationsmustbeinvertible.Inaddition,thecipherandtheinverseciphermustusetheseoperationsinsuchawaythattheycanceleachother.Theroundkeysmustalsobeusedinthereverseorder.Tocomplywiththisrequirement,thetransfor-mationsoccurinadifferentorderinthecipherandthereversecipher,asshowninFigureP.15.

First,theorderofSubNibblesandShiftRowsischangedinthereversecipher.Second,theorderofMixColumnsandAddRoundKeyischangedinthereversecipher.Thisdifferenceinorderingisneededtomakeeachtransformationinthecipheralignedwithitsinverseinthereversecipher.Consequently,thedecryptionalgorithmasawholeistheinverseoftheencryptionalgorithm.Notethattheroundkeysareusedinthereverseorder.



AddRoundKey

AddRoundKey

SubNibbles

InvSubNibbles

ShiftRows

InvShiftRows

MixColumns

Ciphertext

InvMixColumns

Round2

0

Ciphertext:3AD2

Key:2475

Plaintext:1A23

16

16

16

W0−W1

W2−W3

W4−W5

Round1

Round1

Round2

KeyExpansion

KeyExpansion

AddRoundKey

AddRoundKey

AddRoundKey

SubNibbles

InvSubNibbles

ShiftRows

InvShiftRows

AddRoundKey

**678*APPENDIX****PSIMPLIFIEDAES(S-AES)*

**FigureP.15*Cipher****andinversecipheroftheoriginaldesign*

Cipherkey

Plaintext

Inverses

Plaintext

Cipherkey

W

−W

0

1

W

−W

W4−W5

***ExampleP.5***

Wechoosearandomplaintextblock,thecipherkeyusedinExampleP.4,anddeterminewhattheciphertextblockwouldbe:

FigureP.16showsthevalueofstatesineachround.WeareusingtheroundkeysgeneratedinExampleP.4.

**FigureP.16*Example****P.5*

SN:SubNibbles

MC:MixColumns

SR:ShiftRows

ARK:AddRoundKey

Preround

**1**

**A**

K

ARK

=2475

16

**3**

**E**

Round1

**3**

**E**

SN

**B**

**F**

**1**

**8**

SR

**B1MCD8ARK8F2BK**1=B1C4

16

**6**

**3**

**4**

**F**

Round2

**6**

**3**

**4**

**F**

SN

**8DSR**

**B7**

**4**

**B**

K

2

ARK

=5D9916

**3**

**A**

**D**

**2**