امنیت اطلاعات

فصل سوم

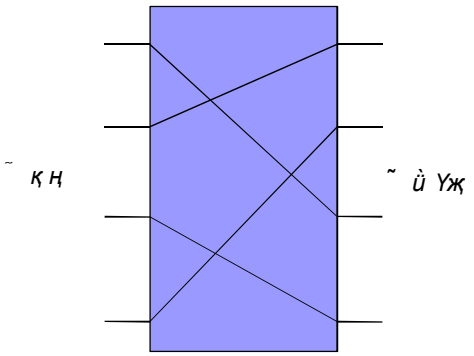
سیستم های نوین رمز متقارن

اجزای اساسی سیستم های مدرن رمز متقارن

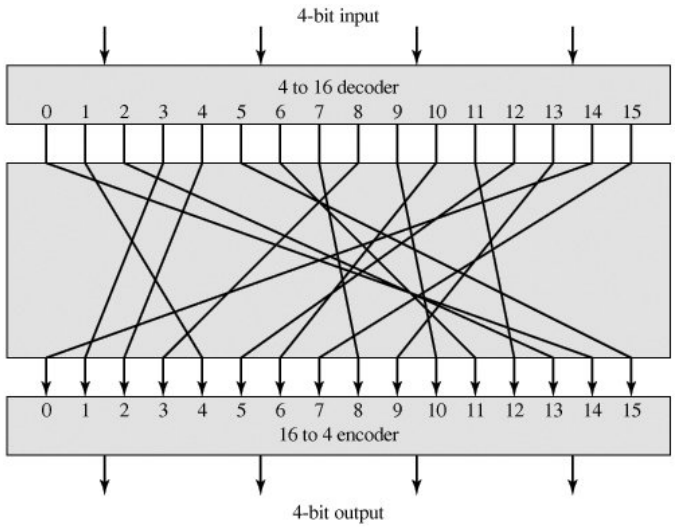
- سیستم های مدرن رمز متقارن عموماً دارای دو جزء اساسی زیر هستند:
  - Permutation Box (P-Box)
    - وظیفه انجام عملیات جابجایی را بر عهده دارد
  - Substitution Box (S-Box)
    - عملیات جانشینی را انجام می دهد

ساختار یک P-Box

- n بیت های ورودی طبق ساختاری مشخص به خروجی می روند



ساختار یک S-Box



انتشار و اغتشاش(گمراه کنندگی)

- هر سیستم رمز متقارن باید دارای دو ویژگی انتشار و اغتشاش باشد
  - انتشار (Diffusion)
    - ساختار آماری متن اصلی باید در حوزه وسیعی از متن رمز شده پخش شود.
    - به بیان دیگر تحلیل آماری متن رمز شده نباید به هیچ عنوان ارتباطی با نتایج تحلیل آماری متن ساده داشته باشد
    - برای ایجاد انتشار باید از تبدیلات خطی استفاده شود که P-Box ها این کار را انجام می دهند.

انتشار و اغتشاش(ادامه)

- اغتشاش (Confusion)
  - نباید بتوانیم هیچ رابطه سرراست و مشخصی بین ورودی ، خروجی و کلید بدست آوریم
  - اغتشاش با تبدیلات غیرخطی ایجاد می شود و S-Box ها این وظیفه را بر عهده دارند

اثر فروپاشی بهمنی

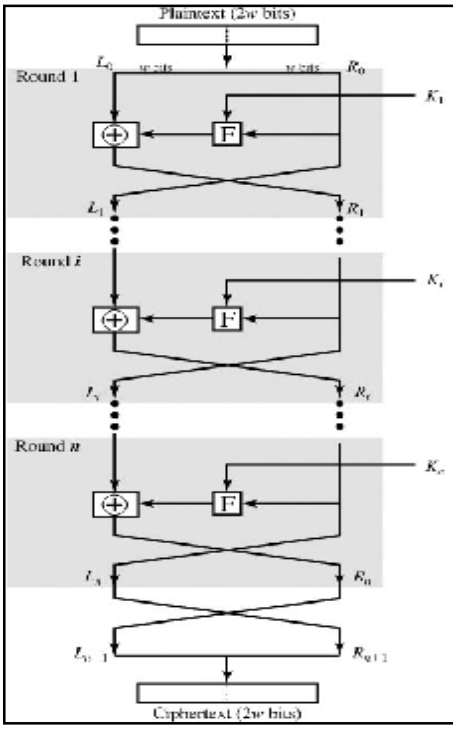
- یکی دیگر از ویژگیهای یک سیستم رمز متقارن قدرتمند، داشتن اثر فروپاشی بهمنی است
  - یک تغییر بسیار جزیی در ورودی یا در کلید (حتی تغییر یک بیت) باید بطور گسترده و غیرمتمرکز و غیرقابل پیش بینی متن رمزشده را تغییر دهد

اصول سیستمهای مدرن رمز متقارن

- سیستمهای مدرن رمز متقارن عموماً از تعدادی دور (Round) تشکیل شده اند
- در هر دور ، یک تابع دور داریم که معمولاً شامل بخش غیرخطی (S-Box) و بخش خطی (P-Box) است.
- در هر دور یک کلید دور استفاده می شود
- کلیدهای دور طبق الگوریتمی مشخص از روی کلید اصلی یا به اصطلاح شاه کلید (Master Key) بدست می آیند

ساختار فیستل

- "هارت فیستل" یکی از پژوهشگران IBM الگویی عام برای رمزنگاری متقارن پیشنهاد داد
- بسیاری از الگوریتمهای نوین رمز متقارن از معماری فیستل تبعیت می کنند.
- طبق یک دسته بندی الگوریتم های متقارن به دو دسته زیر تقسیم می شوند:
  - الگوریتمهای فیستلی
  - الگوریتمهای غیر فیستلی



ساختار فیستل(ادامه)

ویژگیهای ساختار فیستل

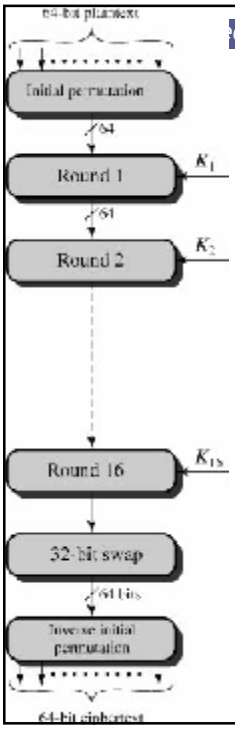
- رمزنگاری از تعدادی دور تشکیل شده است.(معمولاً بین 10 تا 32 دور)
- در هر دور فقط کلید دور و احتمالاً ثابت ها تغییر می کنند و ماهیت عملیات در تمام دورها یکسان است
- ورودی به دو نیمه چپ و راست تقسیم می شود و در هر دور یک نیمه دست نخورده باقی مانده و نیمه دیگر بر اساس ترکیبی بسیار پیچیده و بشدت غیرخطی از نیمه اول و دوم و کلید رمز می شود
- پس از هر دور جای دو نیمه عوض می شود
- کلید هر دور باید متفاوت با کلید دور قبلی باشد

ویژگیهای ساختار فیستل(ادامه)

- کلیدهای دور از روی شاه کلید توسط الگوریتم تولید کلید بدست می آیند
- الگوریتم تولید کلید مستقل از الگوریتم رمزگذاری است
- الگوریتم تولید کلید باید یک الگوریتم یکطرفه باشد
  - یعنی بتوان از روی شاه کلید، کلید های دور را بدست آورد ولی با داشتن کلید های دور نتوان شاه کلید را بدست آورد.
    - چرا؟؟

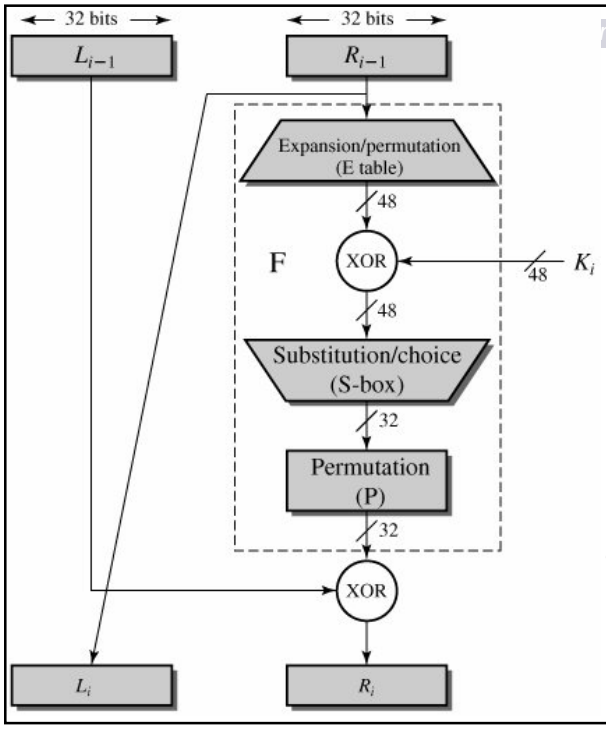
ویژگیهای ساختار فیستل(ادامه)

- طول کلید باید آنقدر زیاد باشد که هیچ کس نتواند با سعی و خطا فضای کلید را جستجو کند.
- امروزه طول کلید های 128، 192 و 256 بیت رایج است
- هر بار یک بلاک داده رمزگذاری و رمزگشایی می شود
- هرچه طول بلاک بیشتر باشد، امنیت الگوریتم بیشتر و شکستن رمز سخت تر است اما از طرف دیگر سرعت الگوریتم کاهش می یابد
- حداقل طول مجاز بلاک داده 64 بیت است ولی در روش های جدید هر بلاک 128 بیت است



الگوریتم DES

- در ابتدای دهه هفتاد دولت فدرال امریکا و شرکت IBM این روش را معرفی کردند.
- مخفف Data Encryption Standard است
- DES از ساختار فیستل پیروی می کند
- ورودی یک قطعه داده 64 بیتی است
- از 16 دور تشکیل شده است
- شاه کلید آن 56+8=64 بیتی و کلیدهای دور 48 بیتی هستند

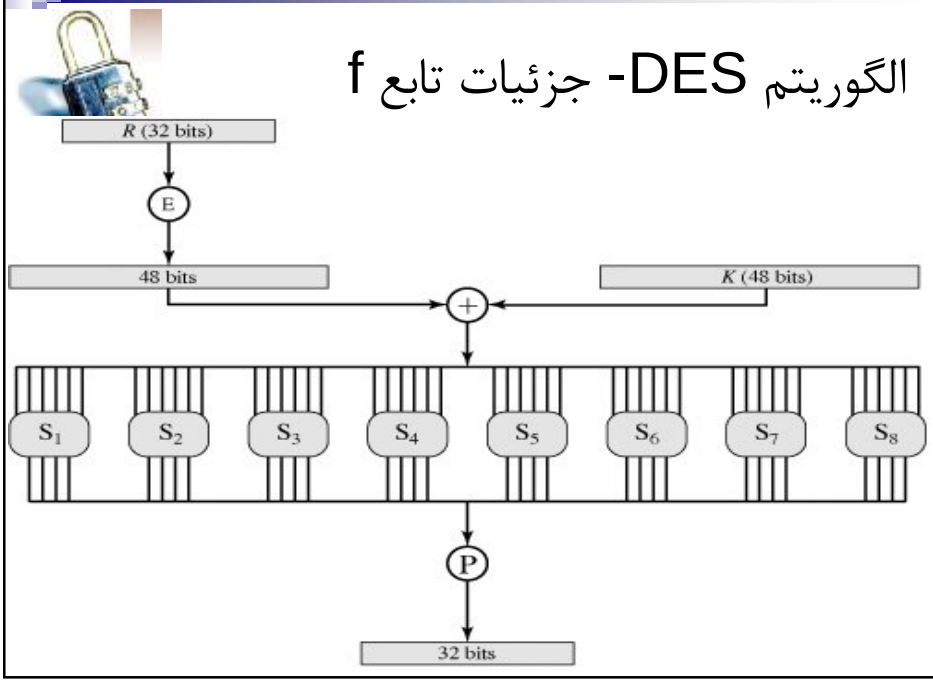


الگوریتم DES (ادامه)

- عملیات انجام شده در یک دور از الگوریتم DES
  - قسمت نقطه چین تابع f را مشخص میکند

15

الگوریتم DES- جزئیات تابع f



الگوریتم DES- جزئیات تابع f(ادامه)

- 32 بیت نیمه راست مرحله قبلی به 48 بیت توسعه می یابند
- نتیجه توسعه با 48 بیت کلید دور Xor می شود
- 48 بیت حاصل xor به هشت قسمت شش بیتی تقسیم می شود
- هر 6 بیت وارد یک S-Box شده و تبدیل به یک 4 بیت می شود
- خروجی s-box ها ، 4*8=32 بیت است
- این 32 بیت وارد یک P-Box می شود
- نتیجه P-Box برابر سمت راست مرحله بعدی است

الگوریتم DES- جزئیات تابع f(ادامه)

- در تابع f و دیگر قسمتهای ساختار DES تعدادی S-Box و P-Box وجود دارد. ساختار این بخش ها ثابت و از پیش تعریف شده است.
- توسعه 32 بیت به 48 بیت:

Expansion Permutation (E)

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Permutation Function (P)

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

- تابع جایگشت (P)

الگوریتم DES- جزئیات تابع f- ساختار داخلی S-Box ها

S_1

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S_2

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S_3

10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S_4

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

19

الگوریتم DES- جزئیات تابع f- ساختار داخلی S-Box ها(ادامه)

S_5

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S_6

12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S_7

4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S_8

13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

20

جزئیات DES

Initial Permutation (IP)

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	61	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Inverse Initial Permutation (IP^{-1})

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

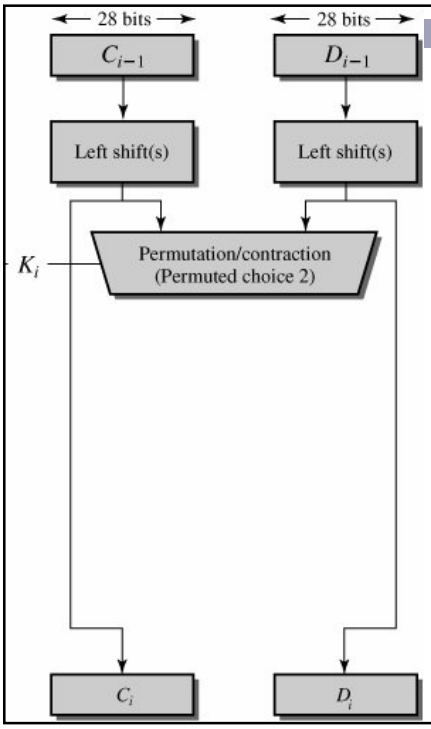
- جایگشت اولیه که قبل از دور اول انجام می شود
- عکس جایگشت اولیه که بعد از دور آخر انجام می شود

21

تولید کلیدهای دور در DES

- همانطور که قبلاً ذکر شد، شاه کلید 56+8=64 بیتی است و باید 16 کلید دور 48 بیتی از روی آن محاسبه شود
- از 64 بیت کلید،
  - 8 بیت آن بیت توازن است و صرفاً برای کشف و کنترل خطا بکار می رود و همان ابتدای فرآیند تولید کلید دور، حذف می شوند
  - اصل شاه کلید 56 بیت است

22



تولید کلیدهای دور در DES(ادامه)

- 56 بیت شاه کلید به دو نیمه 28 بیتی تقسیم شده
- در هر دور تعداد مشخصی شیفت چرخشی به چپ روی هر نیمه انجام شده
- نتیجه شیفت وارد یک P-Box از قبل طراحی شده می شود و کلید دور 48 بیتی از آن خارج می شود

تولید کلیدهای دور در DES(ادامه)

- جزئیات P-Box تولید کلید دور و تعداد شیفت های هر دور

Permuted Choice

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

Schedule of Left Shifts

Round number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bits rotated	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

رمزگشایی DES

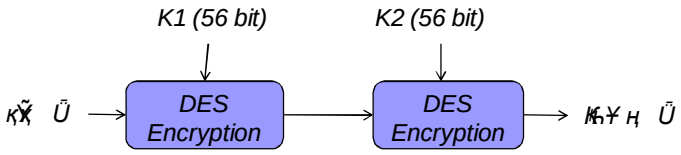
- رمزگشایی نیازی به الگوریتم مجزا ندارد
- فقط کافی است ترتیب کلیدها را برعکس کنیم
  - متن رمزشده را به ورودی الگوریتم می دهیم و کلیدها را به ترتیب عکس رمزگذاری به دورها می دهیم یعنی K_{16} را به دور اول، K_{15} به دور دوم و ... K_1 به دور شانزدهم

استحکام DES

- مهمترین نقطه ضعف قابل توجه DES کوتاه بودن طول کلید آن است
  - در سال 1997 شخصی در مدت 96 روز DES را شکست
  - در سال 1998 الگوریتم DES در 56 ساعت شکست
  - در سال 1999 این الگوریتم فقط 22 ساعت دوام آورد
  - و در سال 2003، نیم ساعت!
- همه این حملات مبتنی بر جستجوی فضای کلید بودند
- تاکنون هیچ نقطه ضعف دیگری در ساختار DES پیدا نشده

Double DES (2-DES)

- برای حل مشکل کوتاه بون کلید، دوبار از DES با دو کلید متفاوت استفاده کردند
- بنابراین طول کلید 112=56*2 بیت شد که طول کلید مناسبی است

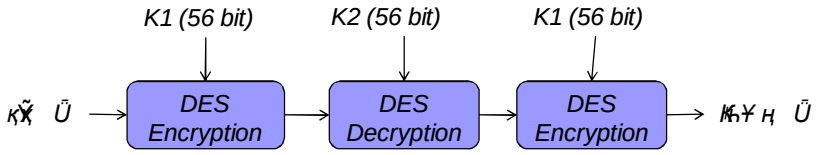


Double DES (2-DES)

- اما مشکل 2-DES
- حمله ملاقات در میانه
  - اگر نفوذگر متن شناخته شده داشته باشد می تواند حمله ملاقات در میانه انجام دهد
    - ابتدا با همه حالات ممکن K1 متن ساده را رمز گذاری میکند
    - سپس با همه حالات ممکن K2 متن رمز شده را رمز گشایی میکند
    - نتایج این دو عملیات در یکی از حالات برابر است که کلید این حالت همان شاه کلید است!
    - پس عملاً دوبرابر کردن طول کلید کمک زیادی به امنیت الگوریتم نکرد

Triple DES (3-DES)

- برای حل مشکل 2-DES تصمیم گرفتند 3 بار از DES استفاده کنند
- 3-DES معمولاً بصورت زیر استفاده می شود:



امنیت 3-DES

- 3-DES با طول کلید 112 بیت غیر قابل شکستن است
- اما
  - شایعاتی پیرامون DES
    - IBM و دولت فدرال امریکا چرا راز هایی از DES را فاش نکردند؟
    - شاید آنها یک کلید فوق سری دارند
    - بنابراین 1000-DES هم فایده ندارد
- پس پیش بسوی AES!

RIJNDAEL / AES

- از سال 1997 تا 2001 رقابتی برگزار شد تا یک استاندارد جدید رمزگذاری مشخص شود
- دو جوان بلژیکی برنده این رقابت شدند Rijmen و Daemen
- ابتدا روش آنها RIJNDAEL نام داشت
- با برنده شدن رقابت، روش آنها Advanced Encryption Standard (AES) نام گرفت
- AES ازلحاظ سرعت وقدرت بسیار برتر از DES بوده و امروزه رایجترین روش رمز متقارن است

AES

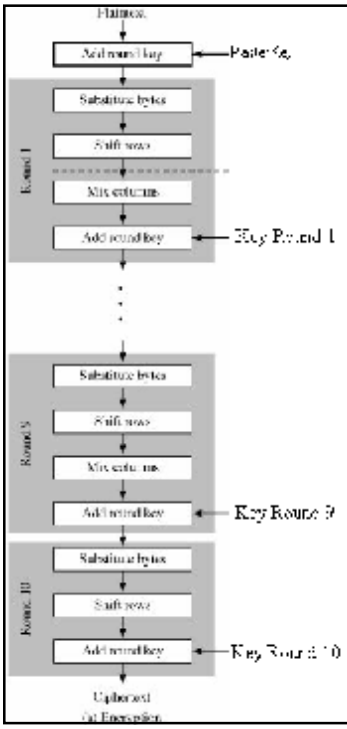
- AES برعکس اکثر الگوریتم های متقارن از ساختار فیستلی تبعیت نمی کند
- AES علاوه بر داشتن امنیت بالا، ساده و سریع است و فضای حافظه کمی نیاز دارد همچنین قابلیت انعطاف زیادی دارد
  - قابلیت انعطاف:
    - در RIJNDAEL طول کلید و طول بلاک داده می توانند 128، 192 و 256 باشند. یعنی به 9 حالت مختلف
    - اما پس از استاندارد شدن آن تعیین شد که در AES طول بلاک داده 128 بیت باشد ولی طول کلید باز هم از بین 128 و 192 و 256 قابل انتخاب است
    - تعداد دورها نیز قابل تغییر است. بین 10، 12 و 14 دور

ساختار AES

- در اینجا نحوه کار الگوریتم AES با طول بلاک و طول کلید 128 و 10 دور را بررسی می کنیم
- الگوریتم در هر دور چهار عمل اصلی زیر را انجام می دهد
  - جانشینی بایت (Substitute Byte)
  - شیفت چرخشی سطرها (Shift Rows)
  - تلفیق ستونی (Mix Columns)
  - اضافه کردن کلید دور (Add Round Key)

ساختار AES(ادامه)

- بر خلاف DES که بر روی بیت ها عمل می کرد، AES بر روی بایت ها کار می کند
- در اینجا بلاک داده و کلید را بصورت یک ماتریس 4*4 در نظر می گیریم که در هر خانه آن یک بایت اطلاعات هست
- آرایه ای که بلاک داده در آن قرار میگیرد را آرایه State گویند



ساختار AES(ادامه)

- در ابتدا متن ساده(آرایه State) با شاه کلید xor میشود
- در دور اول تا نهم هر چهار عمل گفته شده انجام می شود
- بنا بر قرارداد در آخرین دور تلفیق ستونها انجام نمیشود

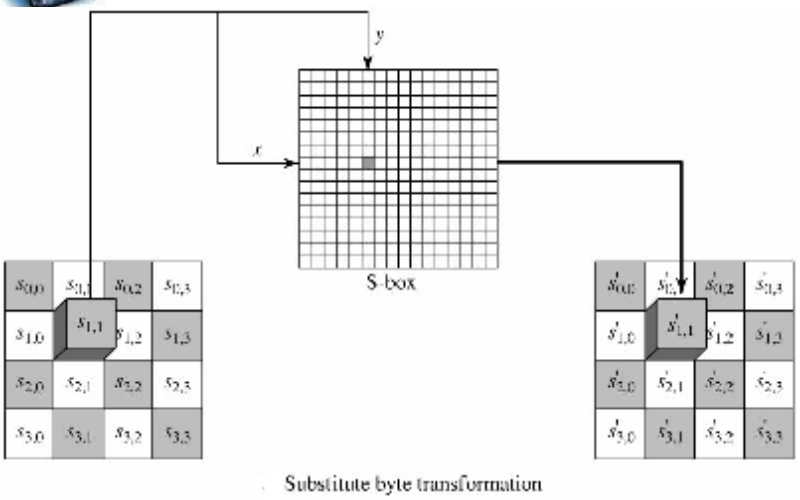
ساختار AES- عملیات جانشینی بایت

- یکایک بایتهای state با مقادیر جدید جایگزین می شوند

S-box

x \ y	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

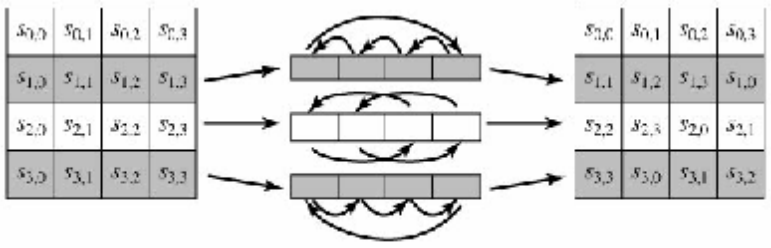
ساختار AES- عملیات جانشینی بایت



Substitute byte transformation

ساختار AES- شیفت چرخشی سطرها

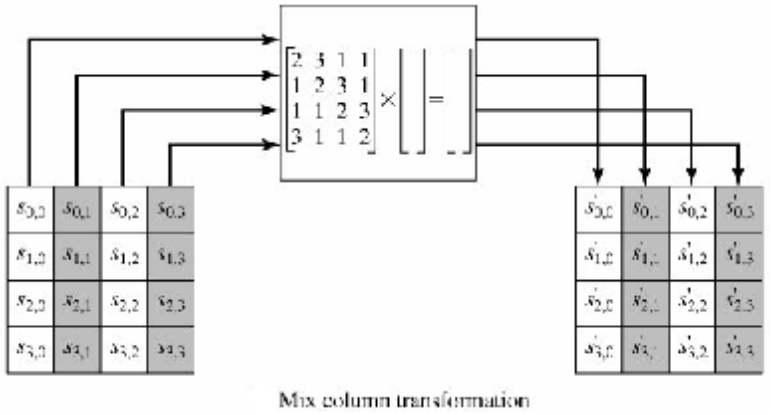
- سطر صفر، نمی چرخد
- سطر یک، یک بایت می چرخد، سطر دو ، دو بایت و سطر سه، سه بایت به سمت چپ شیفت چرخشی پیدا می کند



Shift row transformation

ساختار AES- تلفیق ستونها

- هر ستون از state در یک ماتریس ثابت ضرب می شود

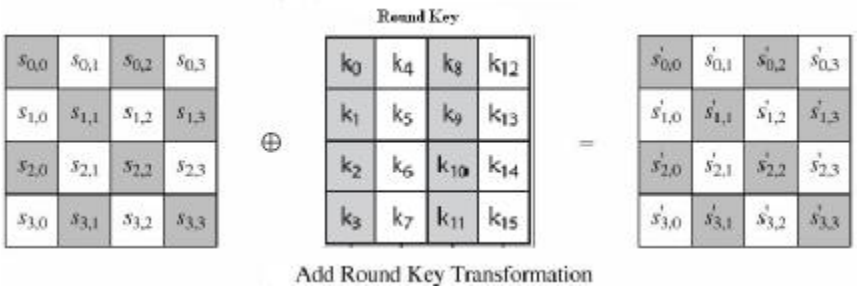


Mix column transformation

39

ساختار AES- اضافه کردن کلید دور

- Xor شدن بایت به بایت کلید دور با state



Add Round Key Transformation

40

رمزگشایی AES

- برای رمزگشایی دقیقاً از همان ساختار رمزگذاری استفاده می شود. فقط ثابت ها تغییر می کنند
  - برای عکس عملیات جانشینی بایت کافی است S-Box را عوض کنیم
  - وارون شیفت چرخشی هم شیفت چرخشی است
  - برای وارون کردن تلفیق ستونها فقط کافی است ستونها در وارون ماتریس قبلی ضرب شوند
  - وارون عمل اضافه کردن کلید دور (xor کلید دور) تکرار عمل xor است

41