به نام خدا

مهندسی اینترنت

فصل ۹
قسمت ۹.۴.۲
روشهای رمزنگاری نوین

تهیه کننده :
فریبا رمضانی

پاییز ۹۳

روش های رمزنگاری نوین

با توجه به ضعف های روشهای جانشینی و جابجایی امروزه دیگر از آنها استفاده نمی شود و در عوض از روشهای ترکیبی جهت بالا بردن بیچیدگی و گمراه کنندگی بیشتر استفاده می شود تا اگر کاشف رمزمتنی رمز شده را در دست داشته باشد نتواند از آن سر در بیاورد.مگر اینکه کلید را داشته باشد.

دو خصوصیت در یک سیستم رمزنگاری:

۱-روش رمزگذاری و رمزگشایی ساده و ارزان قیمت باشد تا افراد مجاز بتوانند به سادگی آنرا داشته باشند.

۲-شکستن متن رمز شده بدون داشتن کلید بسیار مشکل و مقرون به صرفه نباشد.

- **ویژگی های خاص برای الگوریتم ها**

پراکنده سازی(Diffusion):یعنی ساختار و الگوهای آماری متن روی کل متن رمز شده توزیع و پراکنده شود یعنی سیستم نباید ویژگیهای آماری متن(مثل میانگین.واریانس و همبستگی) را به هر نحوی در خروجی رز شده منتقل نماید.و خروجی کاملا تصادفی مستقل از ورودی و غیر قابل پیش بینی باشد.

گمراه کنندگی(confusion):یعنی هیچ رابطه مشخصی بین ورودی و خروجی نباشد و برای رمزگشایی حتی بخش کوچکی از متن بیشتر کلید را بدانیم.

- سیستم های رمزنگاری موفق به دو دسته **کاملا امن** و **با امن محاسباتی** تقسیم میشوند.
- سیتستمی کاملا امن است که کاشف رمز نتواند با داشتن هر سرعت محاسباتی تبدیل های رمزگذاری و رمز گشایی را پیدا کند.
- برای این منظور می توان ابتدا یک رشته بیتی تصادفی را به عنوان کلید انتخاب و سپس متن اصلی بعد از تبدیل به کدی مثل کد اسکی بیت به بیت با این کلید XORنمود.این روش افزونگی یکباره یعنی کلید تصادفی که تنها یکبار استفاده می شود نیز نامیده می شود.
- در سیستم امن محاسباتی کاشف حتی با داشتن قویترین کامپیوترها نمی تواند متن را در کمتر از زمان مشخصی که زمان اعتبار متن است بشکند.

- **تفاوت های رمزنگاری با کدینگ**

در رمزنگاری متن اصلی نباید به طور مستقیم در متن رمز شده باشد.

در رمزنگاری بلوکی یک بیت خطا در ورودی رمزگشا ممکن است بیت های زیادی در بلوک خروجی را تغییر دهد.

در کدینگ بیت های متن به روش سیستماتیک به کد تبدیل می شوند و معمولا بیت های افزونگی مثل توازن نیز اضافه می شود.

در کدینگ سیستم باید بتواند بیشتر خطاهای ممکن را تصحیح کند تا خروجی تحت تاثیر این خطاها قرار نگیرد.

نکته:

دو اصل در رمزنگاری وجود دارد:۱-افزونگی اطلاعات

۲-تازگی

- **الگوریتم های رمزنگاری نوین به دو دسته تقسیم می شوند:متقارن و نامتقارن**

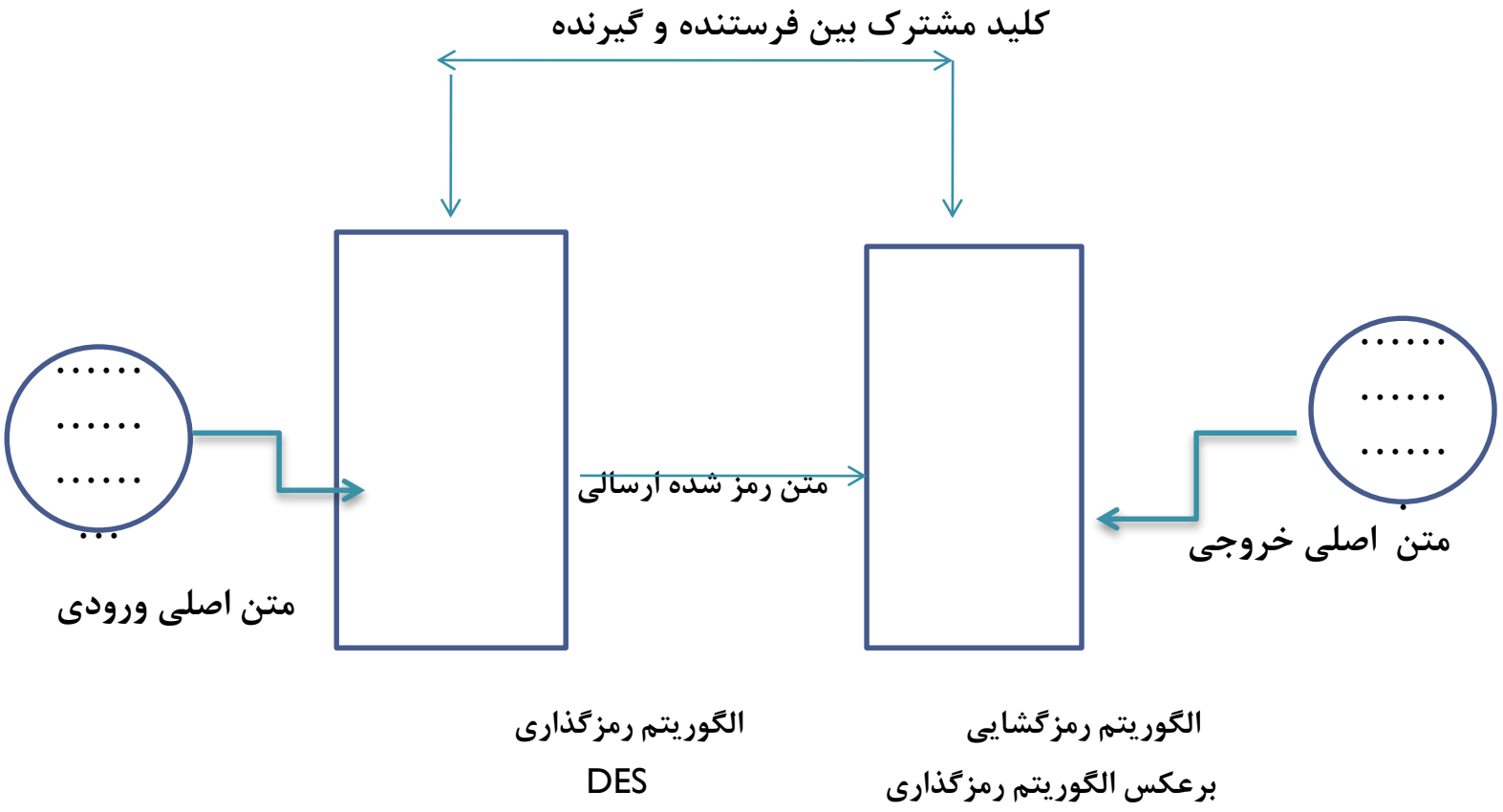
- **متقارن :آنهایی که گیرنده و فرستنده پیام روی یک کلید واحد توافق دارند و آنرا به روشی امن مبادله می کنند.**

- **نامتقارن:آنهایی که کلید رمزنگاری با کلید رمزگشایی فرق دارد و فقط کلید رمزگشایی باید مخفی بماند و کلید رمزنگاری اشکارا اعلام می شود کلید عمومی نیز گفته می شود.**

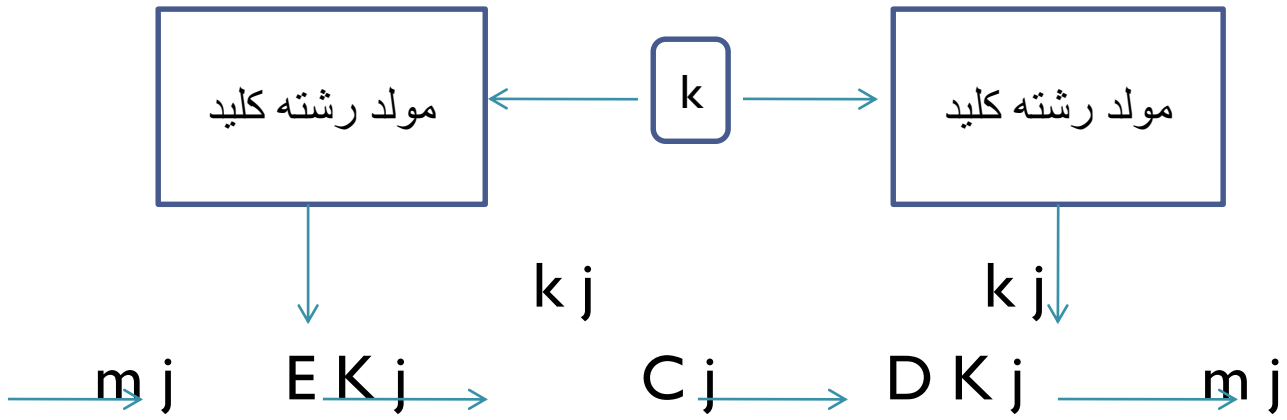
- **رمزنگاری متقارن**
- **در متقارن متن ورودی می تواند بلوکی یا رشته ای باشد.**
- **در روش بلوکی متن اصلی به بلوک های با اندازه ثابت تقسیم می شود سپس هر بلوک بطور مستقل با یک کلید رمز می شود .**
- **اندازه بلوک خا ۶۴ یا ۱۲۸ بیت انتخاب میشود.**
- **مثال:**AES DES

- **در روش رشته ای هیچ بلوکی با اندازه خاص وجود ندارد.**
- **هر بیت متن به نام Mبا امین مقدار کلید K که توسط یک مولد کلید تولید می شود رمز می شود.**
- **در این حالت اگر رشته کلیدPبار تکرار شود متناوب و در غیر اینصورت نامتناوب می باشد.**
- **مثال:ویجنر و ورنام**

رمزگذاری متقارن

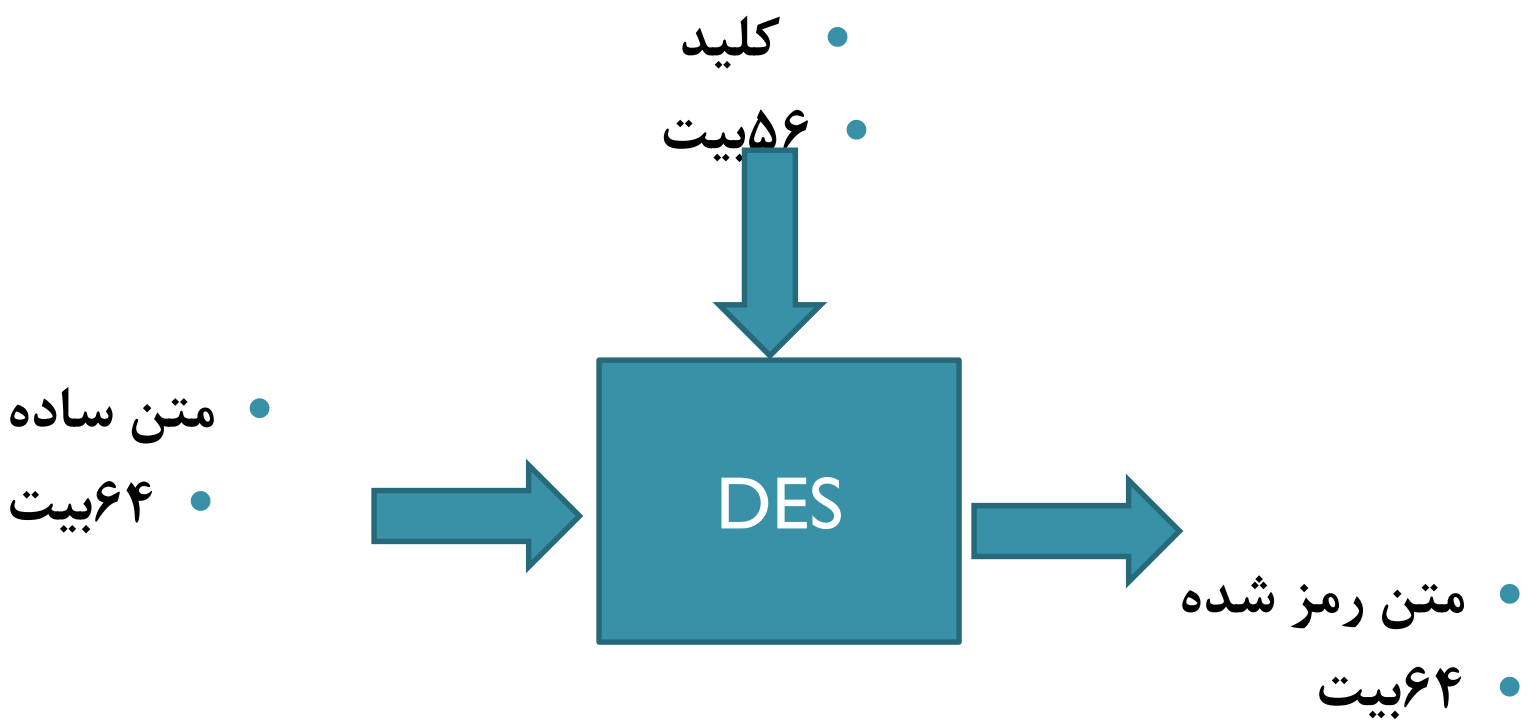


- در رمزنگاری رشته ای اگر رشته کلید بدون استفاده ازمتن اصلی یا متن رمز شده (مستقل از آنها) تولید شود **همزمان** نامیده می شود.
- و اگر به عنوان تابعی از کلید و تعداد مشخصی از متن های رمز شده قبلی تولید شود خود همزمان یا **غیرهمزمان** نامیده می شود.
- و اگر از متن اصلی در تولید رشته کلید استفاده شود **بدون همزمانی** است.



استاندارد رمزنگاری داده ها DES(متقارن)

- در ژوئن سال ۱۹۷۷ دولت آمریکا مولد رمزی را که توسط شرکت IBM ایجاد شد به عنوان استانداردی رسمی پذیرفت.
- یک سیستم رمزنگاری بلوکی با اندازه ۲به توان ۶۴ سیمبل مطابقه شکله زیر درنظر میگیریم.



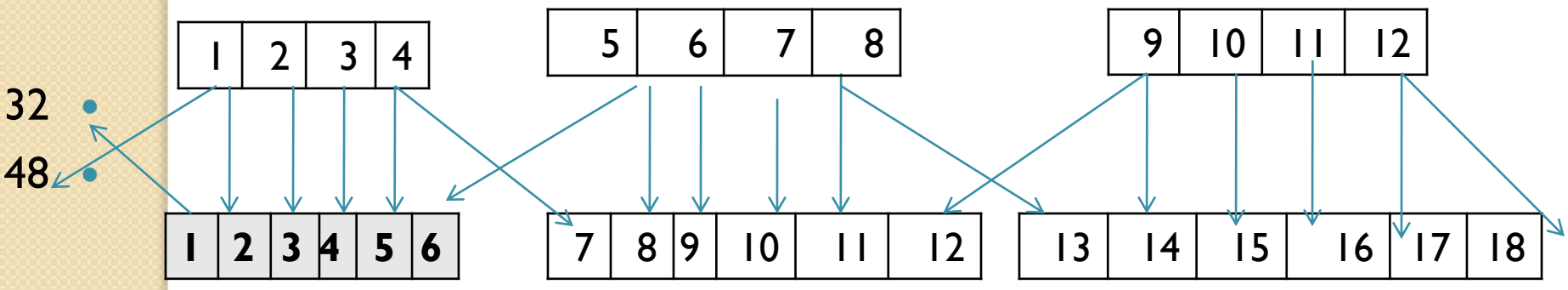
- در استاندارد DESمتن ساده به صورت بلوکهای ۶۴بیتی وارد سیستم شده و متن رمزنگاری شده ۶۴بیتی نیز تولید می شود.این الگوریتم دارای ۱۹مرحله مجزا می باشد.

- مرحله اول و آخر ۳۲بیت چپ را با۳۲بیت راست تعویض میکند و ۱۶ مرحله باقیمانده عملکردی یکسان اما با پارامترهای متفاوت دارند.
- در DES رمزگشایی با همان کلید رمزنگاری صورت می گیرد(متقارن)است.و در این الگوریتم جعبه های جانشینی (s-box)
- و جایگشتی بکار می رود .
- در ابتدا الگوریتم رمزگذاری با یک جایگشت اولیه از ۶۴بیت داده ورودی شروع می کند
- بعد از جایگشت اولیه قلب الگوریتم رمزگذاری در ۱۶مرحله با استفاده از بلوک سازنده استاندارد (SBB)آغاز می شود.

جایگشت اولیه 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	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

جدول توسعه 32بیت به 48بیت با تکرار بیت های کناری



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

- این بلوک از کلید های ۴۸بیتی برای تبدیل ۶۴بیت ورودی به ۶۴بیت خروجی استفاده می کند.
- برای این تبدیل ابتدا ۶۴بیت ورودی به دو قسمت ۳۲بیت چپ و ۳۲بیت راست تقسیم می شود.
- ۳۲بیت ورودی سمت راست Ri-1بدون تغییر به ۳۲بیت سمت چپ خروجی Liکپی می شود و به طور همزمان بر اساس جدول توسعه به ۴۸بیت توسعه می یابند .
- بعد با کلید ۴۸بیتی به صورت مدول دو جمع می شوند.
- جدول توسعه از چپ به راست و از بالا به پایین خوانده می شود که ابتدا ۳۲بیت به بلوک های ۶بیتی تقسیم و هر کدام به ۶بیت تبدیل می شوند ...

- سپس هر کدام از بلوک های ۶بیتی به عنوان ورودی به تابع S-boxعمل نموده و به ۴بیت تبدیل می شوند.توسط این قسمت ۴۸بیت مجدد به ۳۲بیت تبدیل می شود.

- عمل نگاشت:فرض کنید ورودی ۶بیتی هرS-boxرا به صورت b5b4b3b2b1bb0نشان دهید ترکیب بیت اول و اخر از این بیت یعنی b5b0شماره سطر و چهار بیت میانی یعنی b4b3b2b1شماره ستون را در جدول نگاشت مشخص می کنند عددی که در مکان نشان داده شده توسط این سطر و ستون وجود دارد به عنوان خروجی چهار بیتی می باشد.
- ۳۲بیت خروجی حاصل بر اساس جدول جایگشت می شوند خروجی ۳۲بیتی این قسمت با XOR LI-1می شود.

- **الگوریتم بلوک سازنده استاندارد**

$$L_{i-1} = R_{i-1}$$

$$R_i = L_{i-1} (XOR) F(R_{i-1}, K_i)$$

بعد از ۱۶ مرحله تکرار این بلوک ۶۴بیت داده خروجی عکس عمل جایگشتی که در ابتدا انجام شده است را صورت داده تا بیتها سرجایشان قرار گیرند.

انتخاب کلید

- انتخاب کلید نیز در ۱۶ مرحله انجام می گیرد کلبد اصلی شامل بلوک ۶۴ بیتی با ۸ بیت توازن در مکانهای ۸.۱۶...۶۴می باشد.جایگشت اولیه کلید بیتهای توازن را دور انداخته و ۵۶بیت باقیمانده را بر اساس جدول جایگشت می دهد.
- خروجی PC-1به دو قسمت تقسیم می شود CوDکه هر یک ۲۸بیت می باشند الگوریتم انتخاب کلید طی ۱۶ مرحله ۱۶ کلید فرعی ۴۸بیتی برای بلوک های سازنده استاندارد تولید می کنند

جایگشت اولیه pc-1

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

شماره دور	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
تعداد شیفت های چرخشی	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

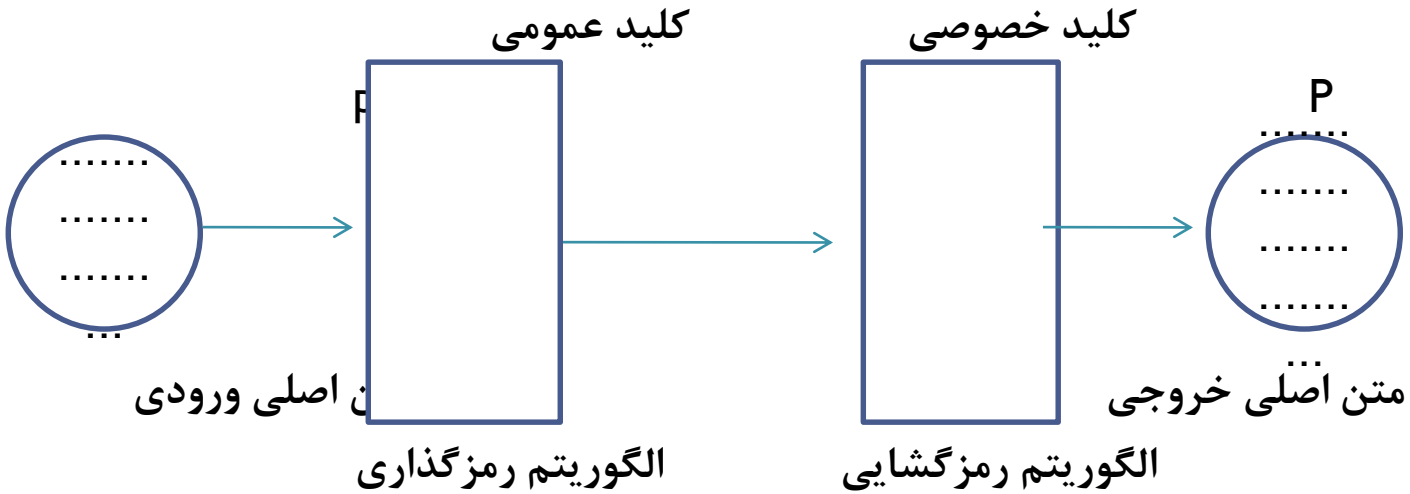
جایگشت ثانویه							
28	3	5	1	24	11	17	14
4	12	19	23	10	21	6	15
2	13	20	27	7	16	8	26
40	30	55	47	37	31	52	41
56	39	49	44	48	33	45	51
32	29	36	50	42	46	53	34

- الگوریتم DESیک سیستم رمزنگاری بلوکی است و عیب ان این است که یک بلوک متنی همیشه به یک متن رمز تبدیل می شود.
- برای عمل رمزگشایی DESمی توان ترتیب کلیدها را معکوس نمود یعنی کلیدهای فرعی K16به K1 را وارد الگوریتم نمود همچنین معکوس عمل های جایگشت را انجام داد .

رمزنگاری نا متقارن(کلید عمومی)

- در سال ۱۹۷۶ دو محقق در دانشگاه استانفورد به نامهای دایفی و هلمن سیستم رمزنگاری جدیدی با دو کلید مجزا (کلید خصوصی یا سری و کلید عمومی) پیشنهاد دادندکه در آن الگوریتم رمزگذاریEو رمزگشاییD باید سه خواسته زیر را براورده سازند:

رمزنگاری نامتقارن



- ۱-D(E(P))=I
- ۲-اشتقاق DازِE بسیار مشکل است.
- ۳-با روش متن ساده انتخابی نمی توان Eرا شکست.

- RSA(نامتقارن)
- در سال ۱۹۷۸ سه نفر به نامهای ری وست.شامیر و آدلمن روش دیگری برای پیاده سازی الگوریتم کلید عمومی با دو کلید عمومی و خصوصی مجزا ارائه دادند.روش انها مبتنی بر بعضی از اصول تئوری اعداد است.
- الگوریتم تولید کد
- دو عدد تصادفی اول بزرگ مثل q, pرا پیدا کنید(۱۰۲۴بیتی معادل ۳۰۹رقم دهدهی)

- مقدارهای n=p*q و z=(P-1)*(q-1) را به دست اورید.
- عدد صحیح e<z را طوری بیابید که نسبت به z اول باشد.
- d<z را طوری پیدا کنید که (e*d)mod z=1 یعنی معکوس حسابی e در پیمانه z محاسبه شود.
- کلید عمومی شامل جفت(n , e) و کلید خصوصی شامل جفت (n , d) می باشد.
- رمزنگاری
- فرستنده A کارهای زیر را انجام می دهد:
- کلید عمومی گیرنده B یعنی (n , e) را به دست می اورد.
- پیام متنی را به صورت یک عدد صحیح مانند m نشان می دهد.
- رمز متن شده را بصورت c=m ^ e mod n محاسبه می کند.
- متن رمز شده c را برای Bارسال می کند.

- رمزگشایی

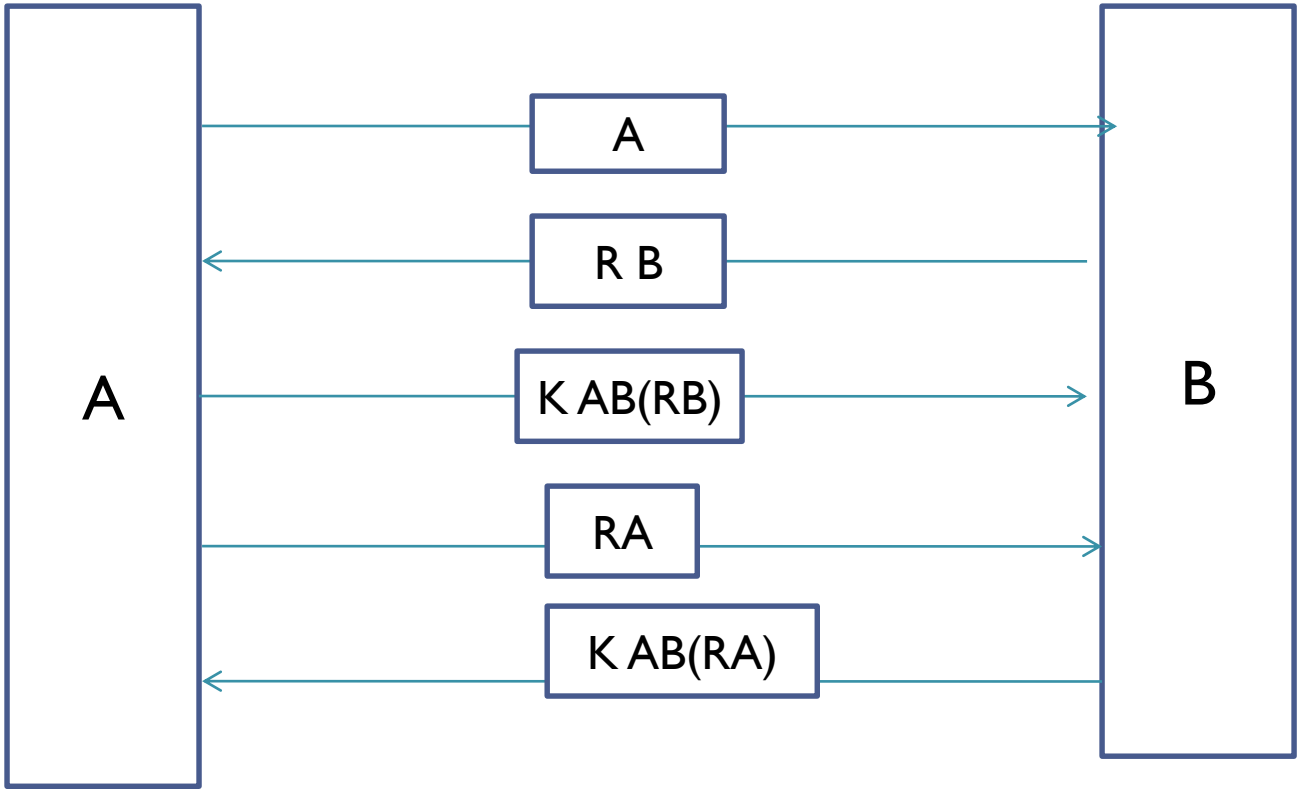
- گیرنده B کارهای زیر را انجام می دهد:
- ۱-از کلید خصوصی (n , d)برای محاسبه m=c ^ d mod n استفاده می کند.
- ۲-متن ساده را از الگوی نمایشی m استخراج می کند.

- **احراز هویت**
- روشی است که با استفاده از ان می توان بررسی نمود ایا مخاطب ارتباط همان کسی است که انتظارش را دارید یا نه.

احراز هویت بر اساس کلید مشترک

- ابتدا Aشناسه کاربری خود را برای Bمیفرستد.
- در پاسخ Bیک عدد تصادفی بزرگ به نام RBتولید و برای Aمیفرستد.
- Aبا استفاده از کلید مشترک عدد دریافتی RBرا بصورت K AB(RB)رمز نموده و برای Bمیفرستد.
- حال Bبا استفاده از کلید رمزگشایی مشترک انرا باز نموده و مطمئن می شود که Aخودش است.
- احرازه هویت دو طرفه است و هویت Bنیز برای Aباید محرز شود.بنابراین Aنیز با تولید یک عدد تصادفی بزرگ Raرا برای Bمیفرستد و در پاسخ Bانرا با کلید مشترک به صورت KAB(RA)دراورده و مجدد برای Aترسال می کند حال هویت Bنیز برای Aمشخص می شود.

- احراز هویت دوطرفه



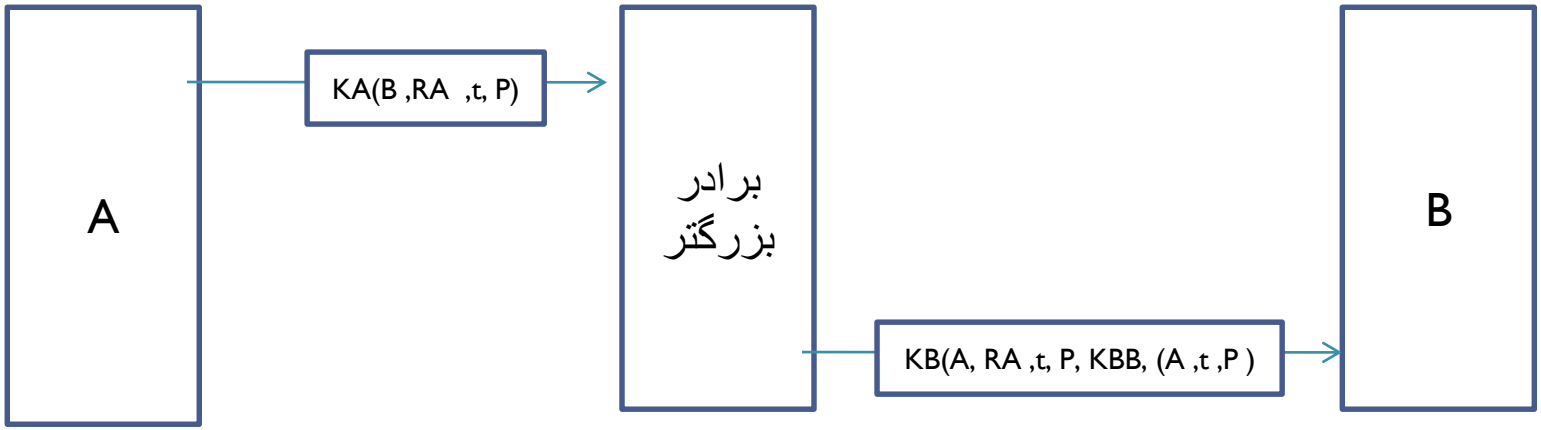
- **امضای دیجیتال**

- در این امضا باید:
- گیرنده بتواند هویت فرستنده را کنترل کند.
- فرستنده بعدا نتواند متن پیام را تکذیب کند.
- گیرنده نتواند خودش پیام را سرهم کند و ادعا کند کس دیگری آن را ارسال نموده است.

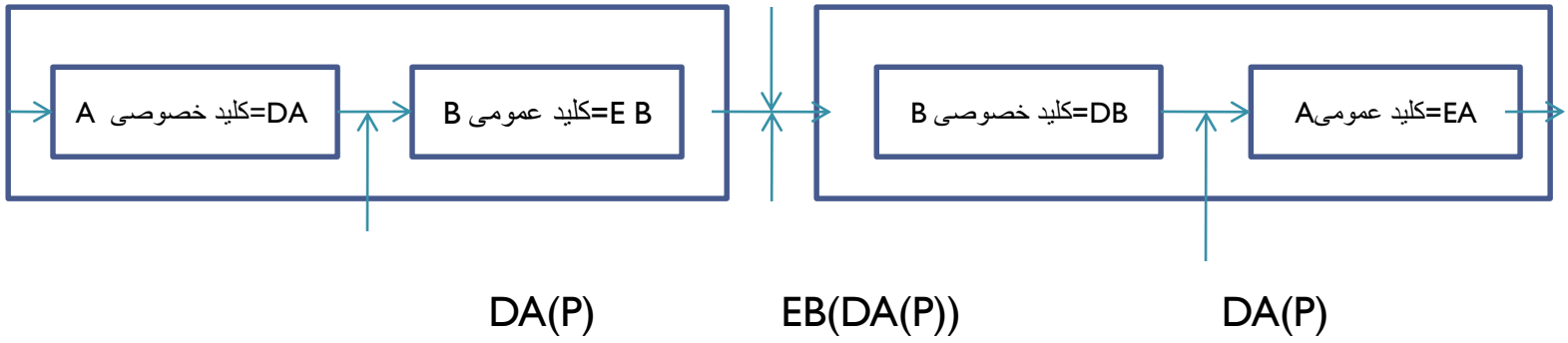
- **امضا با کلید متقارن**

- در این روش یک مسئول مرکزی داریم که همه چیز را می داند و همه به ان اعتماد دارند که این مسئول مانند یک برادر بزرگ است .هر کاربر کلیدی سری را انتخاب می کند و آنرا به دفتر وی تحویل می دهد.فقط A(فرستنده) و برادر بزرگتر رمز یعنی K Aرا می دانند.
- وقتی فرستنده بخواهد پیام ساده امضا شده ای به نام Pرا به گیرنده Bبدهد K A(B, R A ,t ,P)را تولید می کند که Bهویت گیرنده RAعددی تصادفی است که توسط فرستنده انتخاب شده و tزمان ارسال برای اطمینان از جدید بودن پیام و KA(B,R A, t ,P)پیامی است که با کلید فرستنده رمز شده است.

- **امضای دیجیتال با قرار گرفتن فردی با هویت برادر بزرگتر بین فرستنده و گیرنده**



- **امضا با کلید نامتقارن**
- **در رمزنگاری نا متقارن یا کلید عمومی فرض کنید Aبتواند پیام متنی امضا شده ای به نام Pرا با انتقال ((EB (DA (P به Bبفرستد.توجه کنید که Aکلید(اختصاصی)رمزگشایی خودش یعنی D aرا می شناسد ضمن اینکه کلید عمومی یعنی E bرا نیز می شناسد لذا Aمی تواند این پیام را بسازد.**
- **وقتی Bپیام را دریافت می کند انرا به کمک کلید اختصاصی خود تبدیل نموده و DA(P)را بدست می اورد سپس با استفاده ازEAآنرا رمزگشایی نموده و متن اولیه بدست می آید.**



اصول امنیت در یک محیط کاری شبکه

- احراز هویت با استفاده از شناسه کاربری و کلمه رمز.
- نصب ضد ویروس ها و تنظیم بروزرسانی خودکار انها روی همه ی کامپیوترها.
- نصب آخرین وصله های امنیتی و به روز رسانی های امنیتی سیستم عامل و سرویس های موجود.
- گروه بندی کاربران و اعطای مجوزهای لازم به فایل ها و دایرکتوری ها.
- پیکربندی دستگاه هایی مانند مسیریاب سوئیچ و دیواره آتش بر اساس سیاست موجود و توپولوژی شبکه.
- تعیین استرتتژی تهیه پشتیبان از اطلاعات.
- امنیت فیزیکی.
- امنیت سرویس دهنده وب.
- بررسی و تنظیم و آزمایش سیستم های حسابرسی (Auditing)و واقعه نگاری(Logging).
- ایمن نمودن دسترسی از راه دور.
- نصب دیواره های آتش شخصی در سطح میزبان ها برای بالبا بردن امنیت کاربران.
- انجام سرویس های دوره ای تعمیرات جهت افزایش امنیت سخت افزاری.