امنیت اطلاعات

فصل چهارم

رمزگذاری کلید عمومی

رمزنگاری کلید عمومی

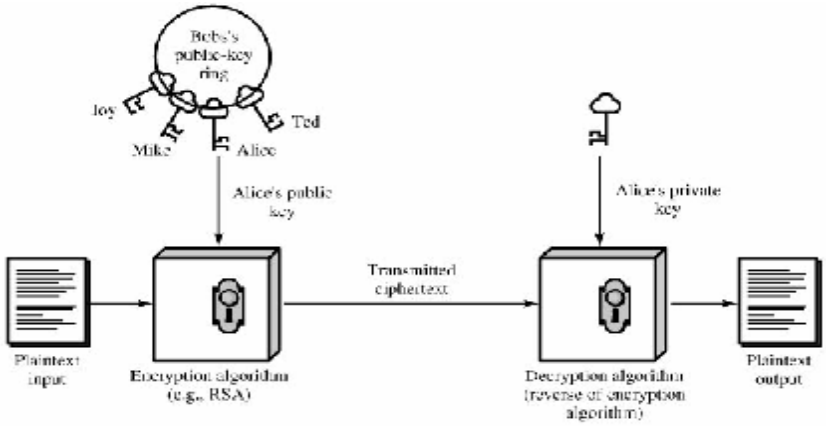
- رمز نگاری:
  - رمزنگاری متقارن
    - از یک کلید یکسان برای رمزگذاری و رمزگشایی استفاده می شود
      - مشکل: فرستنده و گیرنده باید بر سر یک کلید سری به توافق برسند
  - رمزنگاری نامتقارن(کلید عمومی)
    - کلید رمزگذاری و رمزگشایی یکی نیستند.
      - نیازی به توافق قبلی نیست

رمزنگاری کلید عمومی(ادامه)

- در رمزنگاری کلید عمومی هر موجودیت دو کلید دارد
  - کلید عمومی (Public Key)
    - همه آنرا می دانند، چه دوست و چه دشمن.
  - کلید خصوصی (Private Key)
    - فقط خود شخص این کلید را می داند، هیچ فرد دیگری نباید از آن باخبر باشد . حتی افراد مورد اعتماد.
- وقتی داده ها با یکی از این کلید ها رمزگذاری شوند، فقط و فقط با جفت آن قابل رمزگشایی هستند.
  - مثلاً اگر با کلید خصوصی A داده ها رمز شوند، حتی با همان کلید خصوصی هم نمی توانیم آنرا رمزگشایی کنیم، داده های رمز شده فقط با کلید عمومی A قابل رمزگشایی هستند

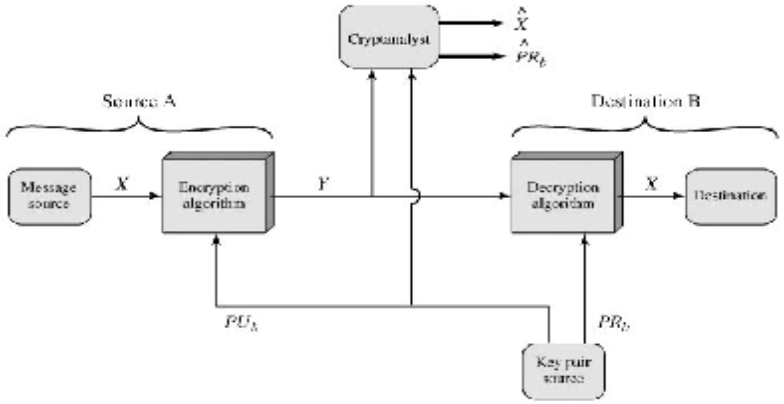
استفاده از رمز کلید عمومی

- حالت اول- برقراری محرمانگی



استفاده از رمز کلید عمومی(ادامه)

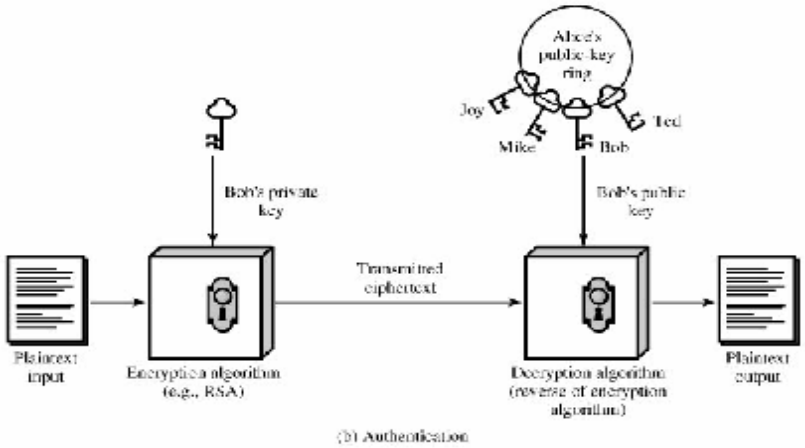
- حالت اول- برقراری محرمانگی



5

استفاده از رمز کلید عمومی(ادامه)

- حالت دوم- برقراری احراز هویت

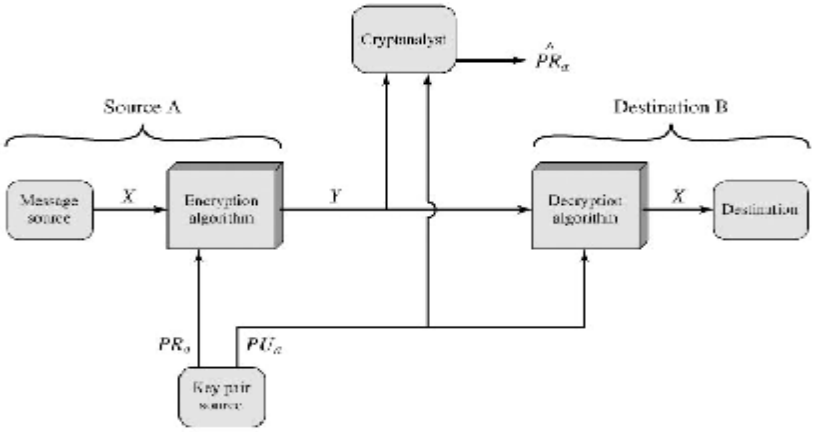


(b) Authentication

6

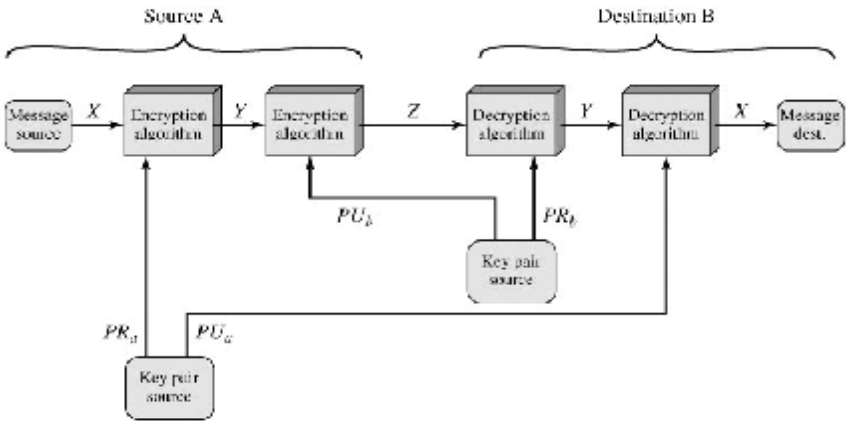
استفاده از رمز کلید عمومی(ادامه)

- حالت دوم- برقراری احراز هویت



استفاده از رمز کلید عمومی(ادامه)

- حالت سوم – برقراری محرمانگی و احراز هویت



اصول الگوریتمهای نامتقارن

- برخلاف الگوریتمهای متقارن که معمولاً مبتنی بر عملیات جابجایی و جانشینی هستند، الگوریتمهای نامتقارن مبتنی بر مسائل غیرقابل حل ریاضی هستند.
- قدرت هر الگوریتم نامتقارن وابسته به سختی و غیرقابل حل بودن یک مساله ریاضی است.
- تابعی که از یک طرف براحتی محاسبه می شود ولی عمل عکس آن غیرممکن است را تابع یکطرفه گویند.
- اگر تابع به گونه ای باشد که با داشتن اطلاعات خاصی معکوس پذیر باشد، این تابع را تابع یکطرفه با دریچه مخفی گویند
- با استفاده از تابع یکطرفه با دریچه مخفی می توان الگوریتم نامتقارن ساخت.

الگوریتم RSA

- در سال 1978 ری وست، شامیر و ادلمن این الگوریتم را معرفی کردند.
- این الگوریتم مبتنی بر سختی مساله "تجزیه یک عدد بسیار بزرگ به عوامل اولش" می باشد.
- کلید عمومی و خصوصی هرکدام یک جفت عدد هستند
  - کلید عمومی (e,n)
  - کلید خصوصی (d,n)
- مشخص است که e,d,n باید با یکدیگر رابطه داشته باشند.
- این رابطه به گونه ای است که با داشتن e,n نباید توانست d را بدست آورد

رمزگذاری RSA

- فرض میکنیم زوج کلید تولید شده و میخواهیم متن ساده را با (e,n) رمز کنیم.
  - متن ساده به بلوک های k بایتی تقسیم می شود($2^k<n<2^{k+1}$)
  - هر بلوک طبق قاعده ای کاملاً دلخواه به یک عدد صحیح به نام P_i تبدیل می شود
  - برای هر بلوک P_i طبق رابطه زیر C_i بدست می آید:
    - $C_i = (P_i)^e \mod n$
  - کدهای C_i بعنوان متن رمزشده ارسال می شوند

تولید کلیدها در RSA

- دو عدد اول دلخواه بزرگ p , q را انتخاب کنید
- n و z را طبق روابط زیر حساب کنید
  - n= p * q
  - z= (p-1)(q-1)
- d را به گونه ای انتخاب کنید که نسبت به z اول باشد (یعنی بزرگترین مقسوم علیه مشترکشان یک باشد)
- بر اساس d، عدد e را به گونه ای انتخاب کن که:
  - $(e * d) \mod z = 1$
- (e,n) کلید عمومی و (d,n) کلید خصوصی هستند

مثال RSA

- تولید کلید:
  - انتخاب p=3 , q=11
  - محاسبه n=33 , z=20
  - انتخاب 7 بعنوان d. (7 نسبت به 20 اول است)
  - برای e اعداد مختلفی می توانیم داشته باشیم. اعداد 3و23و43و63 و ... قابل قبولند که در اینجا e=3
  - بنابراین
    - کلید عمومی (3,33)
    - کلید خصوصی (7,33)

مثال RSA (ادامه)

- حال میخواهیم متن زیر را رمزگذاری کنیم
  - Plain text : cats and dogs
- ابتدا متن ساده را قطعه بندی کرده و به هر قطعه یک عدد می دهیم
- در اینجا به صورت زیر عدد دهی شده:
  - a=00 , b=01 , c=02 , … , z=25

مثال RSA (ادامه)

رمز گذاری				رمز گشایی	
کاراکتر	P_i	P_i^e (e=3)	P_i^e mod n (n=33)	C_i^d (d=7)	C_i^d mod n
C	02	8	08	2097152	02
A	00	00	00	00	00
T	19	6859	28	13492928512	19
S	18	5832	24	4586471424	18
A	00	00	00	00	00
N	13	2197	19	893871739	13
D	03	27	27	10460353203	03
D	03	27	27	10460353203	03
O	14	2744	05	78125	14
G	06	216	18	612220032	06
S	18	5832	24	4586471424	18

15