# مفاهیم امنیت

سپهر مقیسه

دکتر شهریاری

۹۸۳۱۱۰۳

پاییز ۱۴۰۱

۱.از کلید عمومی میتوان برای کد گزاری پیام استفاده کرد اما نمیتوان با همان کلید عمومی پیام را از کدگزاری بیرون اورد و نیاز به وجود کلید مخفی است تا پیام را دیکود کند. نیاز به ذکر است از هر کلید میتوان برای رمزگزاری استفاده کرد. و هرکلید عمومی به یک کلید خصوصی وصل میشود.

۲.میتوان از تابع درهمساز در قسمت f الگوریتم فیستل استفاده کرد و چون این قسمت f هم در decrypt و هم encrypt استفاده میشود ( یعنی دو سویه است ) میتوان از توابع یک سویه مانند توابع درهمساز نیز استفاده کرد. میتوان از آن در مود های ofb و cfb استفاده کرد.

۳.

$M=c^d \bmod n$

$\varphi(N)=4*6=24$

$D=24k+1/5$

$D=5$

$M=10^5 \bmod 35$

$M=5$

۴.

الف)

$9=2^{xa} \bmod 11$

$Xa=6=\text{private key}$

ب)۳

$3=2^{xb} \bmod 11$

$Xb=8$

$K\ ab = 3^8 \bmod 11$

$K\ ab = 5$

۵.

امضاهای دیجیتال در بسیاری از جنبه‌ها مشابه امضاهای سنتی دستی هستند.انجام امضاهای دیجیتال به شکل صحیح بسیار مشکل تر از یک امضای دستی است.طرح‌ها فایل امضای دیجیتال بر مبنای رمزنگاری نامتقارن هستند و می بایست به شکل صحیح صورت گیرد تا موثر واقع شود. برخلاف امضای دستی، پس از امضای دیجیتال سند، هر تغییری در محتوای سند امضاشده به سادگی قابل تشخیص است. بنابراین، امکان جعل یا تغییر اسناد غیر ممکن می‌شود. در واقع هر تغییر در سند، موجب نامعتبر شدن امضای دیجیتال آن می‌شود.

**معایا:**

- الگوریتم و قوانین مربوط به آن نمی‌توانند تاریخ و زمان امضای یک سند را در ذیل آن درج کنند از همین جهت شخص دریافت کننده نمی‌تواند این اطمینان را حاصل کند که نامه واقعاً در چه تاریخ و زمانی به امضا رسیده است.
- چون پیام توسط یک تابع مشخص به مجموعه‌ای از بیت‌ها ترجمه و پردازش می‌شود ممکن است در طی مرحله انتقال و دریافت پیام ترجمه پیام دچار خدشه شود و مفهوم دیگری به خود گیرد. برای حل این مشکل از روشی با عنوان دبلیو وای اس آی دبلیو وای اس استفاده می‌شود به این معنا که همان چیزی که مشاهده می‌شود امضا می‌شود. در این روش همان اطلاعات ترجمه شده خود را بدون آن که اطلاعات مخفی دیگری در آن قرار گیرد امضا می‌کند و پس از امضا و تایید اطلاعات از سوی شخص فرستنده درون سامانه به کار گرفته می‌شود. در واقع این روش ضمانت نامه محکمی برای امضای دیجیتال به شمار می‌رود و در سیستم‌های رایانه‌ای مدرن قابلیت پیاده سازی و اجرا را خواهد داشت .

**مزایا:**

- استفاده از امضای دیجیتال سندیت و اعتبار ویژه‌ای به یک سند می بخشند.وقتی که هر فرد دارای یک کلید خصوصی در این سامانه است با استفاده از آن می‌تواند سند را امضا کرده و به آن ارزش و اعتبار داده و سپس آن را ارسال کند.
- در موارد بسیار زیادی،فرستنده و گیرنده پیام نیاز دارند این اطمینان را به دست بیاورند که پیام در مدت ارسال بدون تغییر باقی‌مانده است.هرچند رمزنگاری محتوای پیام را مخفی می‌کند ولی ممکن است امضا در یک سامانه از اعتبار ساقط شود و محتویات یک پیام دست خوش تغییرات گردد.استفاده از امضای دیجیتال به عنوان روشی از رمز نگاری می‌تواند ضامن درستی و بی نقصی یک پیام در طی عملیات انتقال اطلاعات باشد زیرا همانطور که در ساختار اجرایی شدن الگوریتم مشاهده کردید از تابع درهم سازی بهره گرفته شده است و همین نکته ضمانت بهتری را برای درستی و صحت یک پیام ایجاد می نماید.

.۶

طرح امضای کور پروتکلی است که برای متقاضی این امکان را فراهم می کند تا امضای معتبری را برای پیام خود به وجود آورد بدوناینکه امضا کننده محتوای پیام را ببیند؛ یکی از کاربردهای اساسی امضای کور در رای گیری الکترونیکی می باشد، نکته کلیدی و مهمدر رای گیری الکترونیکی این است که این عمل با استفاده از فن آوری اطلاعات و ارتباطات روند انتخابات را بهبود و سرعت می بخشدو امنیت و صحت این عمل را با وجود یک سرور احراز هویت تضمین می کند، این اطمینان توسط رمز نگاری صورت می پذیرد.

یک طرح امضای کور، پروتکل امضا شامل مراحلی از قبیل کور کردن پیام توسط متقاضی امضا، امضای پیام کور توسط امضا کننده، بازگشایی کوری از امضا و بدست آوردن امضای معتبر توسط متقاضی امضا می باشد. در امضای کور سه خصیصه بنیادی وجود دارد که بایستی برآورده شود: کور بودن پیام، غیرقابل ردیابی بودن و غیر قابل جعل پذیری. کور بودن به این معنی است که متن پیام باید برای امضا کننده غیرقابل مشاهده باشد.
غیرقابل جعل بودن نیز به این معناست که فقط امضا کننده می بایست قادر به تولید امضای معتبر باشد.
غیرقابل ردیابی بودن نیز زمانی برآورده می شود که اگر امضای کور برای عموم آشکار شود، امضا کننده نتواند درخواست کننده امضا را شناسایی کند. امضای کور را می توان با یک مثال ساده توصیف کرد. فرض کنید پیامی را در داخل یک پاکت قرار دهیم و آن را برای امضا به سمت امضا کننده ارسال کنیم. امضا کننده بدون باز کردن پاکت، آن را امضا می کند. این پاکت قابلیت انتقال اثر امضا بر روی پیام دارد. با توجه به اساسی بودن نقش امضای کور در کاربردهایی همچون رای گیری الکترونیکی، پول الکترونیکی؛ طراحی پروتکلی کارآمد با امنیت بالا برای تولید امضای کور برای استفاده در این کاربردها باید مد نظر قرار گیرد.

.۷

N=13*11=143

Phi(n)=120

D=120k+1/11=11

C=3^11 mod 143=113

D=113^11 mod 143=3