1)

الف)

مدیریت کلید فرآیند ایجاد، ذخیره، توزیع و کنترل کلیدهای رمزنگاری برای حفظ امنیت اطلاعات است.

ب)

تهدیدهای مدیریت کلید شامل موارد زیر است:

1. گم شدن کلید :اگر کلید رمزنگاری گم شود، دسترسی به اطلاعات امن غیرممکن می‌شود.
2. سرقت کلید :اگر کلید توسط افراد غیرمجاز به دست آید، امنیت اطلاعات به خطر می‌افتد.
3. سوءمدیریت :استفاده نادرست یا اشتباه در ذخیره‌سازی و توزیع کلیدها.
4. قدیمی شدن کلید :کلیدهای قدیمی ممکن است به مرور زمان آسیب‌پذیر شوند.

ج)

کلید اصلی : کلیدی است که برای تولید سایر کلیدها استفاده می‌شود و معمولاً به صورت طولانی‌مدت نگهداری می‌شود. این کلید برای رمزگذاری کلیدهای موقت یا جلسه به کار می‌رود.

کلید جلسه : کلیدی است که به صورت موقت برای یک جلسه ارتباطی خاص ایجاد و استفاده می‌شود. این کلید برای رمزگذاری داده‌های منتقل‌شده در یک ارتباط امن استفاده می‌شود و معمولاً پس از اتمام جلسه حذف می‌شود.

کاربرد:

کلید اصلی امنیت کلی سیستم را تضمین می‌کند.

کلید جلسه امنیت داده‌های یک جلسه خاص را فراهم می‌کند.

د)

مرحله 1 : درخواست از سوی A (Initiator) به مرجع کلید عمومی همراه با زمان ارسال می‌شود.

مرحله 2 : مرجع کلید عمومی، کلید عمومی B (Responder) و اطلاعات درخواست را رمزنگاری‌شده به A می‌فرستد.

مرحله 3 : A پیامی شامل شناسه خود (IDA) و عدد تصادفی (N1) را با استفاده از کلید عمومی B رمزنگاری کرده و به B می‌فرستد.

مرحله 4 : B نیز درخواست مشابهی به مرجع کلید عمومی همراه با زمان ارسال می‌کند.

مرحله 5 :مرجع کلید عمومی، کلید عمومی A و اطلاعات درخواست‌شده را رمزنگاری‌شده به B می‌فرستد.

مرحله 6 : B عدد تصادفی دریافت‌شده (N1) را با کلید عمومی A رمزنگاری کرده و عدد تصادفی جدید (N2) را اضافه می‌کند و به A می‌فرستد.

مرحله 7 : A عدد تصادفی N2 را با کلید عمومی B رمزنگاری کرده و به B ارسال می‌کند.

2)

الف)

تصدیق هویت (Authentication) : تضمین می‌کند که کاربران و سرویس‌ها هویت واقعی دارند و توسط سیستم شناسایی شده‌اند.

مجوزدهی (Authorization) : اطمینان می‌دهد که کاربران فقط به منابع یا سرویس‌هایی دسترسی دارند که مجاز هستند.

امنیت انتقال داده‌ها : محافظت از داده‌های انتقال‌یافته میان کلاینت و سرور با استفاده از رمزنگاری.

مدیریت کلیدها : توزیع و نگهداری امن کلیدهای رمزنگاری برای ارتباطات امن میان طرفین.

ب)

پشتیبانی از رمزنگاری‌های مختلف:
نسخه 5 از الگوریتم‌های رمزنگاری متنوع پشتیبانی می‌کند، در حالی که نسخه 4 به الگوریتم DES محدود بود.

پشتیبانی از پروتکل‌های شبکه:
نسخه 5 طراحی شده تا در محیط‌های شبکه پیچیده‌تر و پروتکل‌های متنوع) مثل (IPv6 به خوبی عمل کند، در حالی که نسخه 4 محدود به IPv4 بود.

مدیریت زمان:
در نسخه 5 از تایم‌استمپ‌های 32 بیتی به 64 بیتی تغییر داده شده است که امکان استفاده در بازه زمانی طولانی‌تر را فراهم می‌کند.

ساختار پیام‌ها:
پیام‌ها در نسخه 5 انعطاف‌پذیرتر و قابل سفارشی‌سازی‌تر هستند، در حالی که در نسخه 4 ساختار پیام‌ها سخت‌تر و محدودتر بود.

پشتیبانی از چندین حوزه (Realm) :
نسخه 5 توانایی پشتیبانی بهتر از ارتباطات بین چندین حوزه امنیتی را دارد، در حالی که نسخه 4 در این زمینه محدودتر بود.

ج)

در پیام 6، nonce که معمولاً به عنوان t نمایش داده می‌شود برای جلوگیری از حملات تکرار (Replay Attacks)استفاده می‌شود. این nonce به گونه‌ای طراحی شده است که یک پیام خاص را منحصر به فرد کند و تضمین کند که پیام مربوط به یک جلسه یا زمان خاص است nonce .معمولاً یک مقدار تصادفی یا زمان‌سنجی است که تضمین می‌کند حتی اگر مهاجم پیام را رهگیری کند، نمی‌تواند آن را در ارتباطات آینده دوباره استفاده کند.

د)

رمزنگاری nonce به این دلیل انجام می‌شود که از دستکاری آن در هنگام انتقال جلوگیری شود. با رمزنگاری nonce با استفاده از یک کلید مخفی، این اطمینان حاصل می‌شود که فقط گیرنده مورد نظر می‌تواند اصالت آن را تأیید کند و پیام تغییر نکرده باشد. این امر کمک می‌کند تا حملات تکرار جلوگیری شود و صحت و تازگی جلسه تأمین گردد.

۳)

الف)

گواهی کلید عمومی یک سند دیجیتال است که حاوی کلید عمومی و اطلاعات مربوط به هویت صاحب کلید عمومی می‌باشد. این گواهی به صورت یک امضای دیجیتال معتبر شده است و از طریق آن می‌توان از صحت و اعتبار یک کلید عمومی اطمینان حاصل کرد.

این همان کلیدی است که برای رمزنگاری اطلاعات یا تایید امضا استفاده می‌شود. کلید عمومی به صورت یک رشته کد در گواهی قرار می‌گیرد.

نام صاحب گواهی (Subject) : این بخش شامل اطلاعات شناسایی صاحب کلید عمومی است، مانند نام کامل، آدرس ایمیل، یا نام دامنه (برای سرورهای وب).

نام صادرکننده (Issuer) :این بخش مشخص می‌کند که گواهی توسط کدام مرجع صدور Certificate Authority)یا (CA صادر شده است. این مرجع معمولاً باید یک نهاد معتبر در زمینه امنیت اینترنت باشد.

دوره اعتبار (Validity Period): این اطلاعات شامل تاریخ شروع و تاریخ انقضا برای گواهی است. این بازه زمانی مشخص می‌کند که گواهی از چه تاریخی معتبر است و تا چه زمانی می‌توان از آن استفاده کرد.

شماره سریال (Serial Number): این یک شناسه منحصر به فرد برای گواهی است که توسط صادرکننده (CA) برای شناسایی گواهی در پایگاه داده‌های خود استفاده می‌شود.

الگوریتم امضا (Signature Algorithm): الگوریتمی که برای امضای دیجیتال گواهی استفاده شده است، مانند RSA یا.ECDSA

امضای دیجیتال : این امضا توسط صادرکننده گواهی (CA) برای تایید اصالت گواهی و اطلاعات موجود در آن قرار می‌گیرد. این امضا به وسیله کلید خصوصی صادرکننده ایجاد می‌شود.

اطلاعات اضافی : در برخی موارد، گواهی‌ها می‌توانند حاوی اطلاعات اضافی باشند، مانند لیست‌های گواهی‌های لغو شده (CRL) یا مشخصات استفاده از کلید عمومی (مثلاً برای امضای دیجیتال یا رمزنگاری داده‌ها).

ب)

رجع گواهی (CA) یک نهاد معتبر است که وظیفه صدور و مدیریت گواهی‌های دیجیتال را بر عهده دارد. این گواهی‌ها شامل کلید عمومی هستند و برای تایید هویت صاحبان کلید و ایجاد ارتباطات امن از طریق رمزنگاری استفاده می‌شوند.

نقش‌های اصلی

1. تایید هویت CA :هویت فرد یا سازمان درخواست‌کننده گواهی را بررسی می‌کند.
2. صدور گواهی :پس از تایید هویت، CAگواهی دیجیتال با کلید عمومی صاحب گواهی صادر می‌کند.
3. مدیریت گواهی‌ها CA :گواهی‌ها را تمدید و لغو می‌کند و اطلاعات لغو شده را منتشر می‌کند.
4. اطمینان از امنیت CA :با امضای دیجیتال گواهی‌ها، از صحت و یکپارچگی اطلاعات اطمینان حاصل می‌کند.
5. ایجاد اعتماد :گواهی‌های صادر شده توسط CA باعث ایجاد اعتماد در ارتباطات امن می‌شوند.

ج)

مراحل صدور گواهی کلید عمومی:

1. درخواست گواهی

صاحب گواهی (مثلاً یک وب‌سایت یا سازمان) یک درخواست امضا (CSR) ایجاد می‌کند که شامل اطلاعات شناسایی مانند نام، دامنه، و کلید عمومی است.

این درخواست به مرجع گواهی (CA) ارسال می‌شود.

2. بررسی هویت توسط:

CAهویت صاحب درخواست را بررسی می‌کند. این فرآیند می‌تواند شامل تایید مالکیت دامنه، اسناد هویتی یا اطلاعات تماس باشد.

برای گواهی‌های عمومی مانندSSL/TLS ، CAممکن است از روش‌هایی مانند ارسال ایمیل تایید یا بررسی اسناد رسمی برای تایید هویت استفاده کند.

3. صدور گواهی:

پس از تایید هویت، CAگواهی دیجیتال را صادر می‌کند که شامل کلید عمومی، نام صاحب گواهی، تاریخ انقضا، امضای دیجیتال CA و دیگر اطلاعات است.

گواهی به‌طور دیجیتال توسط CA امضا می‌شود تا اصالت و یکپارچگی آن تایید شود.

4. ارسال گواهی به صاحب درخواست:

گواهی صادرشده به صاحب درخواست ارسال می‌شود و می‌توان از آن برای ایجاد ارتباطات امن یا امضای دیجیتال استفاده کرد.

نحوه بررسی اعتبار گواهی کلید عمومی:

1. بررسی امضای دیجیتال:

مرورگرها و سیستم‌های دیگر بررسی می‌کنند که آیا امضای دیجیتال گواهی توسط یک CA معتبر (که در فهرست گواهی‌های معتبر سیستم قرار دارد) امضا شده است یا نه.

اگر گواهی توسط یک CA معتبر امضا شده باشد، به عنوان معتبر شناخته می‌شود.

2. بررسی تاریخ انقضا:

تاریخ شروع و پایان اعتبار گواهی بررسی می‌شود. اگر گواهی منقضی شده باشد، اعتبار آن از بین می‌رود.

3. بررسی لیست گواهی‌های لغو شده:

گواهی‌ها می‌توانند لغو شوند CA .اطلاعات مربوط به گواهی‌های لغو شده را در لیست گواهی‌های لغو شده (CRL) یا از طریق پروتکل OCSP (Online Certificate Status Protocol) منتشر می‌کند.

سیستم‌ها می‌توانند بررسی کنند که آیا گواهی در CRL قرار دارد یا خیر.

4. بررسی مطابقت با اطلاعات:

در صورت استفاده از گواهی برای یک دامنه خاص، بررسی می‌شود که آیا اطلاعات گواهی (مانند نام دامنه) با دامنه مورد استفاده همخوانی دارد یا خیر.

د)

گواهی‌های کلید عمومی (Public Key Certificates) مزایای زیادی دارند که شامل تایید هویت، رمزنگاری امن، امضای دیجیتال و اعتماد عمومی است. این گواهی‌ها به‌طور مؤثر امنیت تبادل کلیدها را از طریق روش‌های زیر تضمین می‌کنند:

تایید هویت :گواهی‌ها هویت فرد یا سازمان را تایید می‌کنند، مثلاً در پروتکل SSL/TLS برای وب‌سایت‌ها.

رمزنگاری امن :کلید عمومی برای رمزنگاری داده‌ها استفاده می‌شود و فقط فرد با کلید خصوصی مربوطه می‌تواند آن را رمزگشایی کند.

امضای دیجیتال :برای تایید صحت و اصالت داده‌ها و جلوگیری از تغییرات در اطلاعات استفاده می‌شود.

اعتماد عمومی :گواهی‌ها توسط مراجع گواهی معتبر (CA) صادر می‌شوند که به آن‌ها اعتبار می‌بخشد.

مدیریت کلید :با استفاده از گواهی‌ها، کلیدها به‌صورت امن تبادل می‌شوند و امکان لغو یا تمدید گواهی‌ها نیز وجود دارد.

ه)

چالش‌ها:

مدیریت گواهی‌ها:

- لغو گواهی‌ها :وقتی یک گواهی به دلایلی مانند افشای کلید خصوصی یا تغییر در اطلاعات صاحب گواهی نیاز به لغو داشته باشد، مدیریت و پیگیری گواهی‌های لغو شده (CRL) یا استفاده از OCSP (Online Certificate Status Protocol) می‌تواند پیچیده باشد.
- تاریخ انقضا :گواهی‌ها معمولاً تاریخ انقضا دارند و باید تمدید شوند، که ممکن است در صورت عدم تمدید به مشکلاتی در ارتباطات امنیتی منجر شود.

حمله‌های man-in-the-middle :

- اگر یک CA به درستی تایید هویت را انجام ندهد یا گواهی جعلی صادر کند، حملات MITM ممکن است رخ دهد. در این صورت، مهاجم می‌تواند ارتباطات بین دو طرف را دستکاری کند.

نیاز بسه ذخیره‌سازی امن کلید خصوصی:

- کلید خصوصی باید در محیطی ایمن ذخیره شود. در صورتی که این کلید افشا یا دزدیده شود، امنیت سیستم به خطر می‌افتد.

هزینه‌ها و پیچیدگی‌ها:

- فرایند صدور، تمدید، و مدیریت گواهی‌های کلید عمومی به منابع و هزینه‌های زیادی نیاز دارد، به ویژه برای سازمان‌های بزرگ.

اعتماد به مراجع گواهی :

- اگر یک مرجع گواهی (CA) مورد حمله قرار گیرد یا اعتبار آن خدشه‌دار شود، امنیت تمام گواهی‌های صادرشده توسط آن CA به خطر می‌افتد.

کاربردها:

SSL/TLS

برای ایمن‌سازی ارتباطات وب (HTTPS) استفاده می‌شود. گواهی‌های کلید عمومی برای تایید هویت وب‌سایت‌ها و رمزنگاری داده‌های بین مرورگر و سرور استفاده می‌شوند.

Secure/Multipurpose Internet Mail Extensions

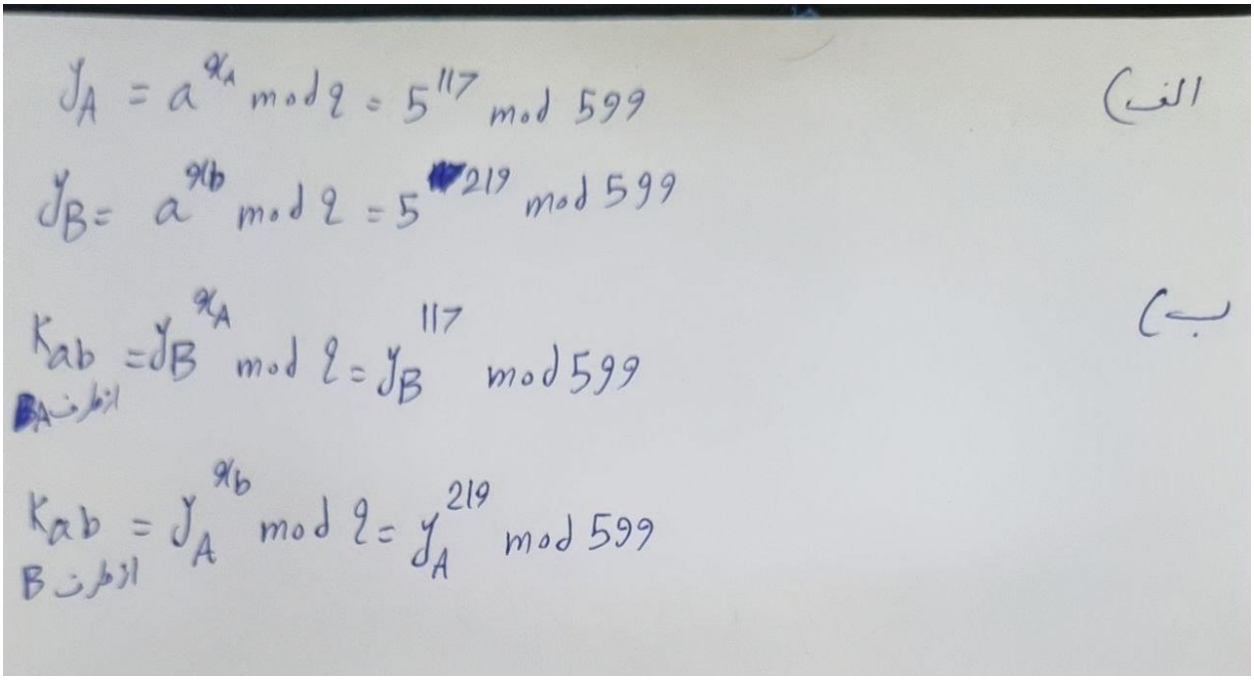
برای رمزنگاری و امضای ایمیل‌ها استفاده می‌شود. این پروتکل از گواهی‌های کلید عمومی برای اطمینان از محرمانگی و اصالت ایمیل‌ها بهره می‌برد.

IPSec

برای رمزنگاری و تایید هویت بسته‌های داده در شبکه‌های IP استفاده می‌شود. گواهی‌های کلید عمومی برای ایجاد تونل‌های امن در ارتباطات شبکه به کار می‌روند.

SSH

برای دسترسی امن به سرورها و سیستم‌ها استفاده می‌شود. گواهی‌های کلید عمومی برای تایید هویت و ایجاد ارتباطات رمزنگاری‌شده بین کلاینت و سرور استفاده می‌شود.



ج)

اگر مهاجم به مقادیر عمومی A و B دسترسی داشته باشد، نمی‌تواند کلید جلسه Kab را محاسبه کند.

دلیل این امر به امنیت الگوریتم دیفی هلمن بستگی دارد. این الگوریتم بر اساس مسئله محاسباتی لوگاریتم گسسته است، که در آن یافتن عدد خصوصی XA یا XB تنها با استفاده از مقادیر عمومی A و B عملی بسیار دشوار است. اگرچه مهاجم می‌تواند مقادیر عمومی را مشاهده کند، اما محاسبه کلید جلسه بدون دسترسی به مقادیر خصوصی (که در اینجا XA و XB هستند) غیرممکن است. این امر به دلیل پیچیدگی محاسباتی در حل معادلات لگاریتم گسسته است که از نظر محاسباتی سخت است.