دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)

Department of
Computer Engineering

به نام خداوند جان و خرد

تمرین تحویلی سوم

درس مبانی امنیت اطلاعات

امیرفاضل کوزه گر کالجی

9931099

سوال اول

- Secure the environment

در این روش، فایل ها و فولدر ها را به گونه ای امن می‌کنیم تا در محیط، اطلاعات حساس لو نروند.

- Encrypt data at rest and in flight

در این روش، تمامی اطلاعاتی که می‌آیند و می‌روند باید توسط یکی از دو روش SSL یا TLS، رمزنگاری شوند.

- Use an authentication and authorization layer

در این روش، یک لایه برای احراز هویت و یک لایه برای اعطای دسترسی به افراد قرار می‌دهیم تا امنیت داده های حساس محفوظ بماند.

- Assign & separate roles

در این روش، نقش ها از یکدیگر به طور متمایز و قابل تشخیص، اعطا می‌شوند و هر کدام از دسترسی های مرتبط با خود برخوردار می‌باشد.

سوال دوم

- Secure
- Reliable
- Transparent
- Scalable

سوال سوم

- در ورژن 5 این سیستم، قابلیت authentication با استفاده از کلید مشترک پیاده سازی شده است. در حالی که در ورژن 4، این مورد پشتیبانی نمی‌شود.
- در نسخه 5، بازه زمانی انقضا تیکت ها را می‌توان بر اساس دقیقه، روز یا ساعت تعیین کرد در حالی که در نسحه 4، این امکان وجود ندارد

- نسخه 5 امکاناتی از جمله posting, renewing, forwarding را در تیکت های خود دارد در حالی که در نسخه 4، این امکانات صرفا به صورت خام قرار داشتند.
- الگوریتم مورد استفاده برای برمزنگاری در نسخه 5، ASN.1 می‌باشد در حالی که در نسخه 4 از الگوریتم receiver makes right استفاده می‌شود.

سوال چهارم

استفاده از کلید جلسه بدین هدف است که، از درخواست های بالا برای ساخت کلید جدید از کلید اصلی جلوگیری شود. بدین صورت، در آن جلسه دیگر نیازی به انتشار تیکت جدید کربروس، به ازای هر درخواست نخواهد بود.

سوال پنجم

در تبادل کلید، یکی از کاربران کلیدی را ایجاد می‌کند و آن را به کاربر دیگر می‌دهد. این روش آسیب پذیری هایی دارد و در برابر حمله ای مانند man in the middle نمی‌تواند مقاوم باشد.

توافق کلید، بدین صورت است که طرفین ارتباط بر سر یک کلید مشترک به توافق می‌رسند. این روش سربار بیشتری دارد زیرا که ابتدای این روش باید ارتباطی اولیه امن ایجاد شود تا طرفین بتوانند بر سر کلید به توافق برسند.

اگر هدف ایجاد ارتباطات طولانی مدت با کاربر دیگر باشد، به نفع است که از روش توافق کلید استفاده شود. اما اگر هدف ارتباطات کوتاه مدت باشد، بهتر است از همان تبادل کلید بهره برد.

سوال ششم

- Session log file
  لاگ های جلسه
- Number of partitions
  تعداد پارتیشن های جلسه
- Source file
  نام فایل مبدا

- Lookup file
نام فایل مورد جست و جو
- Database connection
جزئیات ارتباط با پایگاه داده
- FTP connection
ارتباطی جهت ارسال و دریافت فایل
- Queue connection
یک صف برای نگه‌داری پیام ها

ارتباط میان کلید های عمومی، خصوصی و جلسه در توافق KDC:

1. از کلید های عمومی برای توزیع کلید های اصلی(کلید خصوصی) استفاده می‌شود.
2. از کلید اصلی (رمزنگاری متقارن)، برای توزیع کلید های جلسه استفاده می‌شود.
3. از کلید جلسه برای انتقال امن داده ها استفاده می‌شود.

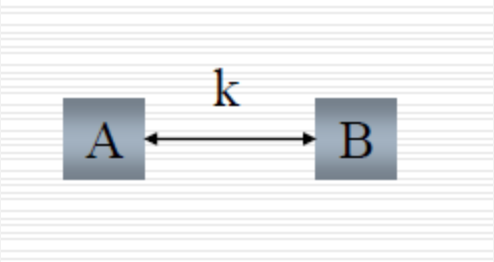
سوال هفتم

از کلید اصلی برای توزیع کلید مخفی جلسه استفاده می‌شود. این کلید بین دو طرفین ارتباط و یک مرکز توزیع کلید یا KDC به اشتراک گذاشته می‌شود. معمولا دستیابی به این کلید، با مراجعه فیزیکی به KDC صورت می‌پذیرد.

دو روش برای توزیع یک کلید بین دو کاربر می تواند روش های زیر باشد:

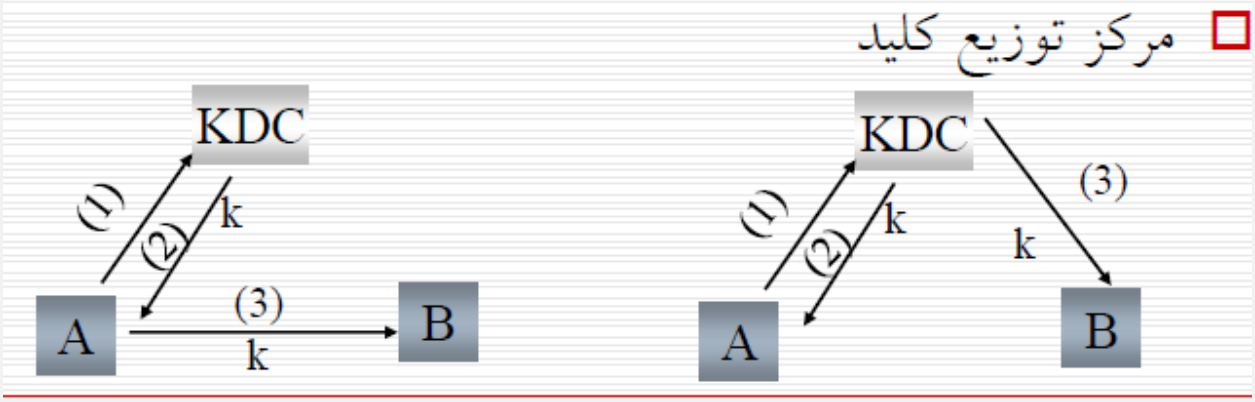
1. نقطه به نقطه:

در این روش تبادل کلید اتفاق می‌افتد و یک کاربر به دیگری کلیدی می‌فرستند و بالعکس:



2. مرکز توزیع کلید:

در این روش از شخص ثالث مورد اعتمادی مانند KDC استفاده می شود تا کلید سری دریافت شود:



~~سوال هشتم(حذف شده)~~

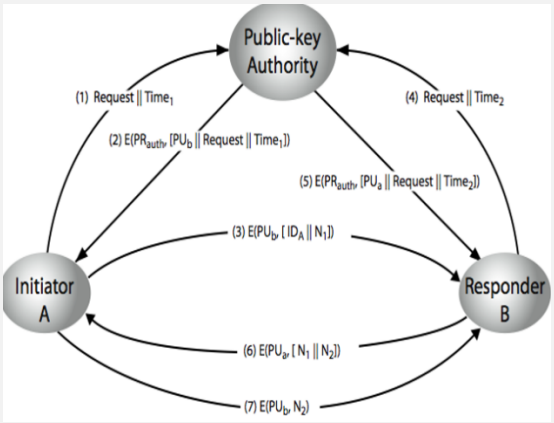
سوال نهم

توزیع کلید های خصوصی با استفاده از کلید های عمومی بدین صورت انجام می‌پذیرد که:

- فرستنده کلید مخفی را با کلید عمومی رمز کرده و به گیرنده می‌فرستد.
- گیرنده محتوای رمزنگاری شده را با کلید مخفی خود رمزگشایی می‌کند.

در یک روش توزیع شده اما، از یک شخص ثالث استفاده می‌شود و طرفین ارتباط به آن شخص ثالث مورد اعتماد درخواست می‌دهند تا کلید عمومی آن کاربر را به دست آورند.

شکل زیر مثال شهودی برای درک بهتر روش متمرکز توزیع کلید می‌باشد:



سوال دهم

الف) برای حل این مسئله داریم:

ابتدا داده ها را می‌نویسیم:

$$\text{A:}\begin{cases} x_A: random \\ y_A: a^{x_A} \bmod q \end{cases}$$

$$\text{B:}\begin{cases} x_B: random \\ y_B: a^{x_B} \bmod q \end{cases}$$

$$k_{A,B} = a^{(x_A \cdot x_B)} \bmod q$$

با توجه به فرمول های نوشته شده و داده های در دسترس برای به دست آوردن X_A داریم:

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

$$x_A = 6$$

ب) ابتدا همانند بخش قبل به دنبال X_B می‌گردیم:

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

$$x_B = 8$$

حال، کلید مشترک را به دست می‌آوریم:

$$k_{AB} = a^{(x_A \cdot x_B)} \bmod q$$

$$k_{A,B} = 2^{6\times 8} \bmod 11$$

$$k_{A,B} = 3$$