آزمایشگاه امنیت شبکه

الگوریتم رمز کلید متقارن AES و مدهای بکارگیری آن

مقدمه: در این آزمایش قصد بر آن است که دانشجویان با نحوه بکارگیری الگوریتم رمز کلید متقارن AES آشنا شوند.

آزمایش ۱-۱: ارسال پیام‌ها به صورت رمز شده روی کانال ناامن

- یک برنامه کلاینت-سرور بنویسید که قابلیت ارسال پیام دوطرفه بین کلاینت و سرور را مقدور سازد.
- با استفاده از این برنامه پیام‌هایی ارسال و دریافت کنید.
- با استفاده از wireshark یا tcpdump ترافیک را شنود کنید.
- یک کلید در اندازه ۱۲۸، ۱۹۲ یا ۲۵۶ بیت تولید کرده و در سمت کلاینت و سرور ذخیره کنید.
- حال برنامه را طوری تغییر دهید که هر پیام قبل از ارسال با استفاده از الگوریتم AES و مد CBC رمزنگاری و پس از دریافت رمزگشایی شود.
- با استفاده از wireshark یا tcpdump ترافیک را شنود کنید.
- اگر بجای مد CBC از مد ECB استفاده کنید آیا تغییری در سطح امنیت پدید می‌آید؟ توضیح دهید.
- فرض کنید ۳۲ ماشین هرکدام با ۸ پردازنده در دسترس است. هر پردازنده در هر ۲۰ میکروثانیه یک عمل تولید کلید و در هر ۹۶ میکروثانیه یک عمل رمزگشایی انجام می‌دهد. اگر در هر ماشین یک پردازنده برای تولید کلید و ۷ پردازنده برای رمزگشایی استفاده شود، در حالت متوسط چقدر زمان نیاز است تا یک متن رمزشده با الگوریتم AES با طول کلید ۲۵۶ بیتی توسط حمله brute force (تولید و تست کلیدها) رمزگشایی شود؟ (فرض کنید یک تابع یک به یک و پوشا بین کلیدها و متون رمزنگاری شده برقرار است و همچنین فرض کنید همگام‌سازی پردازنده‌ها حل شده است.)