امنیت بیشتر با SSL

فهرست‌نویسی براساس اطلاعات فیپا
امنیت بیشتر با SSL
رقیه صمدی ثمرین
(۱۹)ص – مصور – جدول
شابک: ۷-۰۲-۵۹۸۷-۶۰۰-۹۷۸
تهران- علم‌یاران، ۱۳۹۱
موضوع: شبکه‌های کامپیوتری – اقدامات تأمینی - وب – اقدامات تامینی
۱۳۹۱ ۸ الف ۸ ص/ ۵۹ / ۵۱۰۵ TK ۰۰۵/۸ ۲۹۰۷۹۸۶

امنیت بیشتر با SSL

نویسنده:

مهندس رقیه صمدی

چاپ : ادیبی فر

نوبت چاپ : اول – ۱۳۹۱

شمارگان: ۱۰۰۰ نسخه

شابک: ۷-۰۲-۵۹۸۷-۶۰۰-۹۷۸

انتشارات علم یاران

تهران – صندوق پستی : ۱۴۷-۱۴۱۸۵

قیمت : ۲۵۰۰ تومان

امنیت بیشتر با SSL

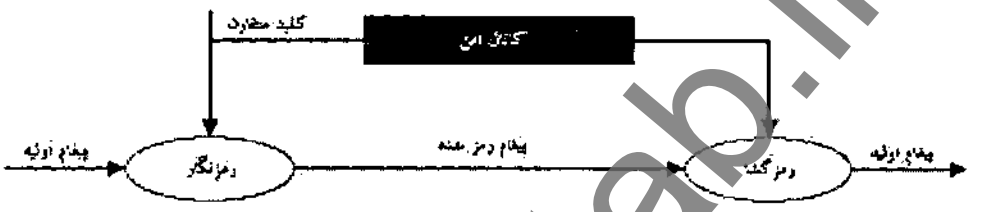
فهرست

۱ مقدمه‌ای بر رمزنگاری

در شبکه‌های باز سه مشکل عمده در زمینهٔ تبادل اطلاعات بین موجودیت‌ها خودنمایی می‌کند. این مشکلات عبارتند از محرمانگی داده‌ها، تمامیت داده‌ها و تایید هویت طرف‌های ارسال‌کننده و دریافت‌کننده. روش‌های رمزنگاری برای فائق آمدن بر این مشکلات طراحی شدند. دو روش رمزنگاری عمده عبارتند از:

- رمزنگاری متقارن[1]
- رمزنگاری نامتقارن[2]

در روش رمزنگاری متقارن کلید رمزنگاری و کلید رمزگشایی هر دو یکسان هستند یا به‌سهولت ازروی هم قابل محاسبه هستند. اولین مشکل این روش تبادل کلید است که باید از طریق یک کانال امن صورت گیرد. مشکل دوم آن است که هر دو موجودیت باید یک کلید مشترک باهم داشته باشند. مشکل سوم نیز سختی ورود موجودیت‌های جدید به سیستم می‌باشد. ازمزایای این روش سهولت پیاده‌سازی و سرعت بالای آن را می‌توان نام برد.



شکل ۲ – رمزنگاری متقارن

در روش رمزنگاری نامتقارن هر موجودیتی دو کلید مرتبط به‌هم با نام‌های کلید عمومی و کلید خصوصی دارد که به‌دست آوردن آنها از روی همدیگر به‌لحاظ محاسباتی‌تقریباً غیرممکن است. داده‌هایی که با یکی از این دو کلید رمز شود با کلید دیگر رمزگشایی می‌شود. کلید خصوصی محرمانه تلقی شده و نزد موجودیت می‌ماند اما کلید عمومی منتشر می‌شود. بنابراین درصورتی‌که دیگران بخواهند اطلاعاتی برایش ارسال کنند که فقط خود وی بتواند بخواند آن را با کلید عمومی‌اش رمز می‌کنند و می‌فرستند. اگر خود آن موجودیت بخواهد پیغامی را امضاء کند آن را با کلید خصوصی‌اش رمز می‌کند و دیگران از کلید عمومی متناظر آن برای بازکردن پیغام استفاده می‌کنند تا مطمئن شوند که پیغام از طرف او بوده‌است. مشکل اصلی این روش تطبیق کلید عمومی با موجودیت است، یعنی بتوان اطمینان حاصل کرد که K کلید عمومی موجودیت X است. برای حل این مشکل زیرساخت کلید عمومی ابداع شد.

[1] Symmetric Cryptography
[2] Asymmetric Cryptography