



مشاوره، تحقیقات، طرح و اجرای شبکه های ارتباطی
و برگزار کننده دوره های آموزشی

ECES

EC-Council Certified Encryption Specialist

اعتبار دهنده: EC-Council

پیش نیاز: آشنایی اولیه با شبکه و امنیت

مدت (ساعت): ۱۶

کاريار ارقام نماينده رسمي شرکت بين المللی EC-Council در ايران

معرفی دوره :

دوره آموزشی ECES مخاطبان را با مبانی و کاربردهای رمزنگاری آشنا می کند. این دوره ضمن بیان تاریخچه و اصول ریاضی رمزنگاری، روند تحول الگوریتم ها را بررسی و شرکت کنندگان را با اصول نظری و عملی این الگوریتم ها آشنا می کند. الگوریتم های رمزنگاری نقش اساسی در بسیاری از راه حل های امنیتی ایفا می کنند. بسیاری از پروتکل های کاربردی در شبکه ها مبتنی بر این الگوریتم ها بنا شده اند. همچنین حفاظت از داده های حساس، احراز هویت، امضای دیجیتال و بسیاری از کاربردها و اهداف امنیتی بدون استفاده از رمزنگاری در دنیای امروز به سختی قابل تصور هستند. در این دوره نگاهی عمیق تر از آنچه در اکثر دوره های آموزشی امنیت وجود دارد، به موضوع رمزنگاری خواهیم داشت. انواع الگوریتم های متقارن و نامتقارن، روش های درهم سازی، اصول ساختاری الگوریتم های رمز و کاربردهای الگوریتم ها از جمله مباحث مطرح در این دوره خواهد بود. همچنین ضمن بررسی و مقایسه استانداردهای رمزنگاری، معیارهای انتخاب الگوریتم های مناسب و نحوه پیاده سازی صحیح رمزنگاری را بررسی خواهیم نمود.

اهداف دوره :

- آشنایی با اصول رمزنگاری
- آشنایی با معیارهای امنیت الگوریتم های رمز و مقایسه آنها
- بررسی کاربردهای رمزنگاری در شبکه و نرم افزار
- کسب مهارت انتخاب الگوریتم های مناسب در کاربردهای مختلف
- آشنایی با پروتکل های امنیتی مبتنی بر رمزنگاری
- آشنایی با حملات علیه الگوریتم های رمز و ابزارهای مربوطه

امتیازات دوره :

- اعطای مدرک فارسی و انگلیسی با مجوز رسمی از :
- مجوز از اداره کل نظام مدیریت امنیت اطلاعات (نما)
- سازمان مدیریت و برنامه ریزی کشور (معاونت توسعه مدیریت و سرمایه انسانی رئیس جمهوری سابق)
- شورای عالی انفورماتیک
- قابلیت ترجمه و تایید قوه قضاییه و امور خارجه
- بهره گیری از لابراتوار سخت افزاری و نرم افزاری مجهز
- بهره گیری از اساتید مجرب و تأیید شده با سابقه حضور در پروژه های ملی
- امکان برگزاری آزمون بین المللی جهت دریافت مدرک بین المللی برای دوره ECES وجود دارد.
- تدریس توسط مدرس رسمی مورد تایید و دارای لایسنس CEI از مرکز رسمی EC-Council

مخاطبان دوره :

- کلیه کارشناسان نرم افزار، شبکه و امنیت و همچنین مدیران فناوری اطلاعات

www.Cdigit.com



« مالکیت مادی و معنوی این مستند منحصراً متعلق به کاريار ارقام است »
لطفاً در باز نشر این مستند نام پدیدآورنده لحاظ گردد.

تهران : خیابان ملاصدرا، بعد از خیابان شیخ بهائی، ساختمان فردوس، پلاک ۲۴۲ تلفن مستقیم آموزش: ۸۸۰۶۲۲۰۳۰۸ فاکس: ۸۸۰۶۵۲۲۲





مشاوره ، تحقیقات ، طرح و اجرای شبکه های ارتباطی
و برگزار کننده دوره های آموزشی

محتوای دوره :	Course Outline :
۱- مقدمه و تاریخچه رمزنگاری a. تعاریف اولیه b. تاریخچه رمزنگاری c. الگوریتم های قدیمی رمز ۲- رمزنگاری متقارن و الگوریتم های درهم ساز a. رمزنگاری متقارن b. مفاهیم رمزنگاری تئوری اطلاعات c. اجزای سازنده الگوریتم های رمز d. معرفی مهم ترین الگوریتم های متقارن e. معرفی مهم ترین الگوریتم های درهم ساز ۳- رمزنگاری نامتقارن a. کاربرد اعداد اول b. عملیات پیمانه ای c. مسائل نظری مربوطه d. تولیدکننده های اعداد تصادفی e. معرفی مهم ترین الگوریتم های رمز نامتقارن f. امضای دیجیتال g. الگوریتم های منحنی بیضوی	۴- کاربردهای رمزنگاری (۱) a. امضای دیجیتال b. گواهی X.509 c. زیرساخت کلید عمومی (PKI) d. الگوریتم های احراز هویت e. پروتکل های VPN f. رمزنگاری g. نهان نگاری ۵- کاربردهای رمزنگاری (۲) a. حملات علیه الگوریتم های رمز b. تحلیل رمز c. انواع روش های تحلیل رمز d. شکستن رمز e. معرفی ابزارها

www.Cdigit.com