Kurs: İnformasiyanın kriptoqrafik mühafizəsi

Kursun müddəti: 5 gün (40 saat)

Kursun proqramı

Modul 1. Kriptoqrafiyaya giriş (2 saat)
İnformasiya təhlükəsizliyinin təmin olunmasında kriptoqrafiyanın rolu. Kriptoqrafiyanın həll etdiyi məsələlər. Kriptoqrafiyanın əsas anlayışları. Kriptoqrafik çevirmələrin növləri. Klassik şifrləmə alqoritmləri. Kriptoqrafiyanın qısa inkişaf tarixi.

Modul 2. Kriptoqrafiyanın riyazi əsasları (8 saat)
Ədədlər nəzəriyyəsindən zəruri məlumatlar. Sadə və mürəkkəb ədədlər. Ən böyük ortaq bölən. Geniş Evklid alqoritmi. Müqayisələr. Çıxıqlar sinfi. Bəzi ədədi funksiyalar. Birməchullu və birdəyişənli müqayisələr. Fermanın kiçik teoremi. Eyler teoremi. Çin qalıq teoremi. Kvadratik çıxıqlar. Lejandr simvolu. Yakobi simvolu. İbtidai köklər. İndekslər və onların xassələri.
Cəbrdən zəruri məlumatlar. Qrup anlayışı. Dövri qruplar. Halqa anlayışı. Meydan anlayışı. Meydanın xarakteristikası. Meydan üzərində çoxhədlilər. Gətirilə bilməyən çoxhədlilər. Meydanın sonlu genişlənməsi. Sonlu meydanların bəzi xassələri. Sonlu meydanların qurulması. Çoxhədlinin tərtibi. Primitiv çoxhədlilər.

Modul 3. Simmetrik şifrləmə alqoritmləri (6 saat)
Blok şifrləri. Feystel şəbəkələri. Blok şifrlərinin rejimləri. DES şifri. QOST 28147-89 şifri. Advansed Encryption Standard (AES). Blok şifrlərinin kriptoanalizi.
Axın şifrləri. Sinxron axın şifrləri. A5 şifri. RC4 şifri. Axın şifrlərinin kriptoanalizi metodları.

Modul 4. Asimmetrik şifrləmə alqoritmləri (6 saat)
Asimmetrik kriptoqrafiyanın əsas anlayışları. Biristiqamətli funksiyalar. Diffi-Hellman sxemi.
RSA şifrləmə sistemi. RSA kriptosisteminin təhlükəsizliyi. RSA parametrlərinin seçilməsi.
Miller-Rabin sadəlik testi. Miller-Rabin testi əsasında sadə ədədlərin generasiyası.
Diskret loqarifmləmə məsələsi. Əl-Qamal şifrləmə sistemi.
Elliptik əyrilərin tərifi. Qrup qanunu. Elliptik əyri üzərində diskret loqarifm məsələsi. ECDSA rəqəm imzası sxemi.

Modul 5. Kriptoqrafik heş funksiyalar (4 saat)
Kriptoqrafik heş-funksiyaların təyinatı, növləri və xassələri.
Heş funksiyaların qurulmasına yanaşmalar. MD5. SHA-1. SHA-2 heş funksiyaları. QOST P34.11-94. Heş-funksiyaların kriptoanalizi.
Məlumatı autentikasiya kodları. Blok şifrlər əsasında MAC. HMAC. MD5-MAC.

Modul 6. Rəqəmsal imza (6 saat)
Rəqəmsal imzanın əsas xassələri. Rəqəmsal imzanın növləri.
RSA imza sxemi. Əl-Qamal imza sxemi. Şnorr imza sxemi. DSA alqoritmi. QOST R34.10.94 imza sxemi. Fiat-Şamir imza sxemi.
Məlumatı bərpa etməklə imza sxemi. Nyuberq-Ryuppel İmza sistemi.
Xüsusi imza sxemləri. Kölgəli imza sxemi. Qrup imzası. İnkarolunmaz imza sxemi. Rəqəmsal imza sxemlərinin təhlükəsizliyi.

Modul 7. İdentifikasiya və autentifikasiya (4 saat)
Əsas anlayışlar və təriflər.
Zəif autentikasiya. Çoxdəfəlik parollar əsasında autentikasiya. Fiksə edilmiş parol sxemləri. Birdəfəlik parollar.
Sertifikatlar əsasında autentikasiya. İstifadəçilərin biometrik identifikasiyası və autentikasiyası.
Ciddi autentikasiya. Simmetrik və asimmetrik şifrləmə sistemləri əsasında "sorğu-cavab".

Sıfır bilik verməklə autentikasiya protokolları. Fiat-Şamir protokolu. Feyc-Fiat-Şamir identifikasiya protokolu. Şnorr autentikasiya protokolu.

Modul 8. Kriptoqrafik açarların idarə edilməsi (4 saat)

Açarların uzunluğunun seçilməsi. Açarların generasiyası. ANSI X9.17 standartı üzrə açarların generasiyası. Açarların saxlanması. Açarların məhv edilməsi. Ehtiyat açarlar. Açarların paylanması. Simmetrik şifrləmə əsasında açarların ötürülməsi. Asimmetrik şifrləmə əsasında açarların ötürülməsi.

Açıq açarlar infrastukturu. Açıq açarlar infrastukturun fəaliyyətinin prinsipləri. Açıq açarlar infrastukturun baza arxitekturaları. Açıq açarlar infrastukturun məntiqi strukturu və komponentləri