ODTÜ UME ÇALIŞMA GRUPLARI

21 Mart 2019

Lattice Attacks against weak ECDSA Signature in Cryptocurrencies

Esra YENİARAS
MEB
(15:00)

CAN(Controller Area Network) Üzerinde Kimlik Doğrulama Protokolü

Sarp MERTOL
ASELSAN
(15:45)

4 Nisan 2019

AES Square Attack

Didem DEMİRBAĞ
Yüksek Lisans Öğrencisi
(15:00)

On CryptGenRandom and Rand/Srand

(Random Number Generators of Windows and C++)

Sermin ÇAKIN
Yüksek Lisans Öğrencisi
(15:45)

18 Nisan 2019

İstatistiksel rastgelelik testleri ile güvenli anahtar üretimi
Aycan USLU
Doktora Öğrencisi
(15:00)

Lineer Cryptanalysis of DES
Cansu BOZKURT
Yüksek Lisans Öğrencisi
(15:45)

ODTÜ UME ÇALIŞMA GRUPLARI

2 Mayıs 2019

Kafes tabanlı kriptografi
İrem KESKİNKURT
Doktora Öğrencisi
(15:00)

Independence and sensitivity of randomness test suite
Gizem KARA
Yüksek Lisans Öğrencisi
(15:45)

16 Mayıs 2019

Kafes Tabanlı Kriptosistemler için Hızlı Polinom Çarpımı
Yusuf Alper BİLGİN
ASELSAN
(15:00)

Yan Kanal Saldırıları ve Koruma Yöntemleri
Damla ÇENESİZ
FAME
(15:45)