Kriptoloji Eğitimi İçin Yazılımlar ve Projeler

Hamdi Murat Yıldırım

Bilkent Üniversitesi,
Bilgisayar Teknolojisi ve Bilişim Sistemleri Bölümü
hmurat@bilkent.edu.tr
www.bilkent.edu.tr/~hmurat/

30 Nisan 2013
ANKARA KRİPTOLOJİ SEMİNERLERİ
YER: ODTÜ KRİPTOLOJİ LAB

Amaç

- Kriptolojiye giriş eğitiminde ve araştırmalarda kazandığı bazı tecrübeleri paylaşmak
  - Verdiğim ders:

    “CTIS 496 Hesaplamada Veri Güvenliği”

  - İçeriği
- Kriptolojide yazılım kullanımının önemine değinmek ve bazılarını tanıtmak
- Kaynaklar ve örnek öğrenci projeleri sunmak

Başlıklar

- Cryptool Portal
- Cryptool 1
- Sage Matematik yazılımı
- gmp kütüphanesi
- Openssl
- Gnu PG
- Bouncy Castle API (Java ve C#)
- Diğer Yazılım projeleri
- Projeler (X.509 sertifikası oluşturma; S/MIME ve PGP e-posta şifreleme/imzalama, v.b.)
- Kaynaklar

Cryptool Portal

- Cryptool (Cryptography for Everybody -Herkes için Kriptografi)
- Portal (http://www.cryptool.org/en/) 5 projeyi çatısı altında topluyor:

- Cryptool 1 http://www.cryptool.org/en/cryptool1

- Cryptool 2 http://www.cryptool.org/en/cryptool2

- JCryptool http://www.cryptool.org/en/jcryptool

- Cryptool Online http://www.cryptool-online.org/

- MysteryTwister C3 http://www.mysterytwisterc3.org/en/ (test your own knowledge by solving a variety of cryptographic challenges.)
- Hangi yazılımda hangi kriptografik fonksiyonlar gerçekleştilmiş?

  http://www.cryptool.org/en/ctp-documentation-en/ctp-functions-en

Cryptool 1 (CT1)

- Yaygın kullanılan, kriptoloji e-öğrenme yazılımı.
- Katkıda bulunanlar: http://www.cryptool.org/en/ctp-team-en
- Geliştirilmeye 1998 yılında başlandı *
- Amaç, kriptografinin ağ güvenliği tehditlerine karşı nasıl yardımcı olacağını ve kriptografinin temel konularını anlatmak *
- Özgür ve açık kod kaynaklı
- C++ ile geliştiriliyor. Visual Studio 2010 geliştirme ortamı.
- Windows İşletim sistemi için geliştirilmiş
- winehq (http://www.winehq.org/) yardımıyla büyük oranda Linux üzerinde çalıştırmak mümkün.

* http://en.wikipedia.org/wiki/CrypTool

Cryptool 1 (CT1) Yetenekleri

- Birçok klasik ve modern kriptografik algoritmalar
- Bazı algoritmaların görselleştirimi: Sezar, Enigma, RSA, Diffie-Hellman, dijital imza, AES, vb.
- Bazı algoritmaların kriptanalizleri
- Kriptanalitik ölçüm metotları (entropy, n-grams, autocorrelation, vb.)
- Bir kısım ek yöntemler: asallık testleri, çarpanlara ayırma, base64 kodlama, vb.
- Sayılar Teorisi kılavuzu
- Kapsamlı çevrim içi yardım
  http://www.cryptool-online.org/

Cryptool 1 (CT1)

- Başlarda kurum için bilgi güvenliği eğitim yazılımı olarak tasarlandı.
- Resmi Sunu Dosyası "Practical Introduction to Cryptography and Cryptanalysis: Scope, Technology, and Future of CrypTool"

  http://www.cryptool.org/images/ct1/presentations/CrypToolPresentation-en.pdf
- Şifreleme Eğitiminde Açık Kaynak Kodlu Araç Kullanımı: Cryptool, Akademik Bilişim 2010, http://ab.org.tr/ab10/kitap/guzel_yuksel_AB10.pdf
- Bir blog yazısı: http://kriptoloji.net/cryptool
- Bir video: http://www.youtube.com/watch?v=PLCzzj9a2Xg
- Cryptool yazılımının kullanıldığı bir lab çalışması:

  http://teal.gmu.edu/courses/ECE646/labs/CRYPTOOL_LAB_F06.pdf
- Cryptool kullanan bir ders: CTIS 496 Hesaplamada Veri Güvenliği, Bilkent Üniversitesi

Cryptool 1 (CT1)
Kurulum ve Canlı Gösteri

- İndirme Sayfası:
  http://www.cryptool.org/en/ct1-download-en

- Kurulum birkaç ileri adımı tıklamakla, kolay.

- 30 Nisan 2013, Salı itibariyle en son sürüm 1.4.31 Beta 8 ile canlı gösteri....

Cryptool 1 (CT1) Desteklenen Diller

- CrypTool 1.4.31: İngilizce ve Almanca
- CrypTool 1.4.30: İngilizce, Almanca, İspanyolca, Lehçe, Sırpça. Yunanca ve Rusça için çalışmalar var.
- Aralık 2012, Ocak 2013 gibi Cryptool Türkçe desteği için CTIS 496 dersini alan öğrenciler ile çalışma başlatıldı:

  https://code.google.com/p/cryptool1-turkish/

  Yapılanlar:

  - Geliştiriciler ile Türkçeleştirme çalışmaları için temas kuruldu
  - Kaynak kodlar, çevrim içi depodan indirilip, incelendi.
  - Hangi dosyalar üzerinde çevirin nasıl yapılacağı tesbit edildi. Başarılı, temel denemeler yapıldı fakat bundan sonra ilerleme kaydedilmedi.
  - Desteğinizi bekliyoruz...

Sage Matematik Yazılımı

- Sage Nedir? Neden Sage?
- Sage'nin Yapısı ve Özellikleri
- Çalışan Örnekler (Canlı gösterim)

Sage Nedir? Neden Sage?

- Sage (Software for Algebra and Geometry Experimentation) : http://sagemath.org
- Lisans: GNU Genel Kamu Lisansı (GPL)
- Sage, çoğu GPL lisanslı birçok
  - özgür ve açık kod kaynaklı yazılım paketleri (GMP, Python, Common Lisp, Bzip2, FreeType,MoinMoin, Wiki,v.b.)
  - matematik yazılımları (Maxima, GAP, Singular, NTL,
  - PARI/GPv.b.) bir şemsiye altında toplayan bir
  - matematik yazılımıdır.
- Matlab,Mathematica, Maple ve Magma gibi ticari matematiksel yazılımlar için özgür ve açık kod kaynaklı bir alternatiftir.

Sage'nin Yapısı ve Özellikleri

- Detaylar:

  Açık Kod Kaynaklı ve Özgür Matematik Yazılımı: SAGE (Sunum)

- Web bağlantıları

  http://www.bilkent.edu.tr/~hmurat/SAGE/

- Çalışan Örnekler (Canlı gösterim)

Sage Kaynaklar

- TEZ, “Exploring Cryptography Using the Sage Computer Algebra System”, Minh Van Nguyen
  - Klasik Kriptosistemler,
  - RSA, Basitleştirilmiş DES, Mini AES şifre sistemleri
- E-kitap, “Cryptography”, David R. Kohel
  - Klasik Kriptosistemler, alıştırmalar
- TEZ, “Algorithmic Algebraic Techniques and their Application to Block Cipher Cryptanalysis”, M. Albrecht
  - Grobner Basis Algoritmaları, örnekler mevcut
  - Araştırmada Sage'nin nasıl kullandığına iyi örnek

    W

Sage Kaynaklar

- “The Sage Project: Unifying Free Mathematical Software to Create a Viable Alternative to Magma, Maple, Mathematica and MATLAB”, Burçin Eröcal and and William Stein

- Sayılar Teorisi ile ilgili (Web Bağlantı)
- Kitap: “Elementary Number Theory: Primes, Congruences, and Secrets”

  -İndirilebilir e-kitap, sage örnekleri mevcut: http://wstein.org/ent/ent.pdf
- Video: Math 480 Sage course -- computational number theory 1
- Eğitimde Sage Kullanımı

Sage'nin Yapısı ve Özellikleri

- Detaylar:

  Açık Kod Kaynaklı ve Özgür Matematik Yazılımı: SAGE

  (Sunum)

- Web bağlantıları http://www.bilkent.edu.tr/~hmurat/SAGE/

- Çalışan Örnekler (Canlı gösterim)

- Örnek Kodlar (8 örnek dosya, sws uzantılı, sage matematik yazılımında açılabilir ve kullanılabilir).

GMP Büyük Sayı Kütüphanesi

- Proje Sayfası: http://gmplib.org
- Wikipedia Girdisi: http://en.wikipedia.org/wiki/GNU_Multiple_Precision_Arithmetic_Library
- Örnekler
  - Çarpma: http://www.bilkent.edu.tr/~hmurat/gmp/carpma.c
  - Miller-Rabin primality test (C, GMP)
  - GMP-ECM (Elliptic Curve Method)

GMP Büyük Sayı Kütüphanesi -Alternatifler-

- GNU MPFR Kütüphanesi,
  - GMP tabanlı ve GMP kodlarını ile çalışmak mümkün.
  - Windows üzerinde kurulumu ve diğer uygulamalarla birlikte kullanımı GMP kütüphanesine göre daha kolay (Teşekkürler, Çağdaş Çalık)
  - Sage matematik yazılım MPFR kullanıyor.
- Nessie projesinde sunulan bir liste

  http://www.cosic.esat.kuleuven.be/nessie/call/mplibs.html

- CRYMPIX: KRİPTOGRAFİK ÇOK-BASAMAKLI KÜTÜPHANE

Openssl

- OpenSSL, SSL ve TLS protokollerinin açık kod kaynaklı gerçekleştirmesidir.
- Temel programlama kütüphanesi C diliyle yazılmıştır, temel kriptografik fonksiyonları gerçekleştirir ve birçok yararlı araç sağlar.
- Bu kütüphanenin diğer birçok programlama dilinde kullanımı mümkün kılan ara yazılımlar mevcuttur

  (http://en.wikipedia.org/wiki/OpenSSL)
- openssl komut satırından kullanımı mümkündür.
  - Örnekler: http://www.madboa.com/geek/openssl/

GnuPG

- GnuPG, RFC4880 ile tanımlanan OpenPGP standardının bir tam ve özgür gerçekleştirmesi olan GNU projesidir.
- GnuPG, veriyi imzalamayı, imza doğrulamayı, veri şifreleme/deşifrelemeyi ve anahtar yönetimini sağlar ve açık anahtar dizinlerine erişimi mümkün kılan modüller ile gelir. (http://www.gnupg.org)
- GNUPG Belgeleri
  - http://www.gnupg.org/documentation/howtos.en.html
  - http://www.gnupg.org/gph/en/manual.html
  - http://wiki.openskills.org/OpenSkills/GPG+Signing+and+Encrypting

GnuPG ve PGP

- Kriptografik algoritmaların, gizliliğin, bütünlüğün ve inkar edilememezlik gibi güvenlik hedeflerinin sağlanmasında nasıl kullanıldığını öğrenmek Için en etkili yollardan biri PGP ye çalışmak:
  - Chapter 7, Network Security Essentials,Stallings
    http://kurser.iha.dk/ee-ict-master/tisgrau01/nse/pp/Chapter-07.ppt
  - Mozilla Thunderbird ve eklentisi enigmail ile şifreli ve/veya imzalı e-posta mesajları gönderme deşifreleme ve/veya imza doğrulama işlemlerini öğreten proje vermek

Bouncy Castle Kripto Uygulama Programlama Arayüzüleri (UPA)

www.bouncycastle.org

- Java (J2ME den JDK 1.6) ve C# programlama dilleri için UPA ailesi
- Java'da 269,000 satır kod, test kodları dahil
- Destek: PKCS#10, PKCS#12, CMS, S/MIME, OpenPGP, TLS, OCSP, TSP, CMP, CRMF ve Attribute Certificates.
- Bitirme projeleri ve gerçek hayat projeleri için önerilir
- Kitap: Beginning Cryptography with Java
  - Örnek kodlar

Diğer Yazılımlar

- Çağdaş Çalık'ın yazılımları:

  anf2weight, CIDAT (Cipher Design and Analysis Tool), FolderHash, BFW, Boolean Function Search,...

  http://www.metu.edu.tr/~ccalik/software.html
- Tools for Cryptography, European Network of Excellence in Cryptology II

  http://www.ecrypt.eu.org/tools/
- Algorithmic Cryptanalysis

  http://www.joux.biz/algcrypt/Programs.html
- Ganzúa: A cryptanalysis tool for classical ciphers

Örnek Öğrenci Projeleri

- CTIS 496 Projesini inceleyelim.
  - S/MIME X.509 Sertifikaları,

    E-posta şifreleme/deşifreleme ve imzalama/doğrulama
  - Gnu PG;
  - Openssl (X.509 sertifika oluşturulması v.b.)
  - Bouncy Castle ve gmp kütüphanesi kullanımı

Diğer Öğrenci Projeleri

- Alptekin Küpçü'nün tavsiyesi (teşekkürler)
  - SEED projesi

    http://www.cis.syr.edu/~wedu/seed/index.html
  - Kitap: “Introduction to Computer Security”, Goodrich and Tamassia, bu projeyi kullanıyor:

    http://www.securitybook.net/
  - (E-posta şifreleme, PGP, openssl, v.b.) http://www.securitybook.net/home/projects
- Kitap: “ Cryptography and Network Security: Principles and Practice (5th Ed.), Stalling
  - Birçok sage matematik projelerine ve Java Kriptografi UPA lerinin kullanıma yer verilmiş.

Öğrenci Projeleri

Hatırlatma, Yıl 1998: the Electronic Frontier Foundation (EFF) tarafından yapılan DES cracker (takma isim " Deep Crack") makinası

- Amaç: DES anahtar uzunluğunun yeterli güvenlik sağlamadığını kanıtlamak. “İnsan gözüyle görünce inanır”

  Öğrenci projeleri, kriptoloji eğitimde öğrenilenlerin iyi kavramak ve kriptografik algoritmalarını uygulanabilir olduğunu göstermek adına önemli ve değerli.

- Maliyet: $250,000 daha az
- Sonuç: DES gizli anahtarlarına 56 saatte ulaşıldı

Öğrenci Projeleri

- Projelerde kullanılacak yazılımların kurulumu, kullanımı konusunda kısa da olsa açıklamalar yapılmalı ve öğrencilerin doğrudan ilgili kriptoloji başlığına odaklanması sağlanmalı.

- Bu tür projeler eğitim başlıklarını işlemeden önce öğrenci motivasyonunu arttırmak adına ödev olarak verilebilir.

Kaynaklar

- Kitap, “Cryptography, An Introduction”, N. Smart

  (Çevrim içi erişim, 3. Baskı)

  İlk baskının bulunduğu Türkiye'den kütüphaneler

  (Tavsiye eden Çağdaş Çalık, teşekkürler)
- Kitap, “Information Security: Principles and Practice”, M. Stamp

  M. Stamp Video Dersleri (Youtube)

  (Tavsiye eden Cüneyt Sevgi, teşekkürler)
- Çevrim içi Ders, coursera.com, “Cryptography I”, D. Boneh

  (Tavsiye eden Halil Kemal Taşkın, teşekkürler)