Şifreleme Eğitiminde Açık Kaynak Kodlu Araç Kullanımı: CrypTool

Elem Güzel[1], Ulaş Yüksel[1], Erkan Yılmaz[1], Gökhan Dalkılıç[1]

[1] Dokuz Eylül Üniversitesi, Bilgisayar Mühendisliği Bölümü, İzmir

elemguzel@gmail.com, ulasyuksel.tr@gmail.com, erkan986@gmail.com, dalkilic@cs.deu.edu.tr

Özet: Şifreleme, güvenlik alanında uzmanlaşmak ve/veya konuya giriş yapmak isteyen öğrenciler ya da profesyoneller için önemli konu başlıklarından biridir. Altında yatan matematiksel teori nedeni ile şifreleme eğitiminde zorluklar yaşanabilmektedir. Görsellikle desteklenmiş bilgisayar uygulamaları, bu alandaki öğretme ve anlama sürecini kolaylaştırabilmektedir. Bu bildiride şifreleme içerikli bir derste, açık kaynak kodlu CrypTool yazılımının eğitim ve geliştirme sürecinde kullanımı ele alınmıştır.

Anahtar Sözcükler: Şifreleme, Kriptografi, Eğitim, Açık Kaynak, CrypTool.

Open Source Tool Usage in Teaching Cryptography: CrypTool

Abstract: Cryptography is one of the important topics for the students and professionals willing to succeed in or to make an introduction to security. Because of the underneath mathematical foundations, some difficulties can be faced during cryptography education. The software tools with visualization abilities may support and improve teaching and learning processes in this field. This paper represents the usage of an open-source software in cryptography oriented course, CrypTool software, in education and development.

Keywords: Cryptography, Teaching, Education, Open Source, CrypTool.

1. Giriş

Bilişim teknolojileri, iletişim ve bunlara yakın alanlarda çalışacak olan mezunlar, bilgisayar ve ağ güvenliği konularında artan oranlarda bilgi birikimine ihtiyaç duymaktadır. Bilgisayar ve ağ güvenliği konularının önemli bir başlığını "şifreleme" oluşturmaktadır [1,2]. Şifreleme içerikli dersler, yukarıda belirtilen ihtiyaca yönelik olarak, "güvenlik" alanında öğrencileri yetiştirmek amaçlı kullanılabilmektedir [1,3]. Aynı zamanda, bu derslerin, genel öğretimde, matematiksel temelleri yerleştirebilmek için kullanılabileceği de düşünülmektedir [4,5].

Dokuz Eylül Üniversitesi, Bilgisayar Mühendisliği Bölümünde lisans ve lisansüstü programlarda "şifreleme" içeriğine sahip üç seçmeli ders bulunmaktadır. Derslerde tahta ve slaytlar üzerinden yapılan anlatımlar yanında, şifreleme algoritmaları ve iletişim kuralları, verilen programlama ödevleri ile pekiştirilmeye çalışılmaktadır. Bu ödevler ve anlatımlarda yardımcı ortam olarak ücretsiz ve açık kaynak kodlu CrypTool eğitim uygulaması da kullanılmaktadır.

Bu bildiride CrypTool'un eğitimde kullanımı ve edinilen tecrübeler paylaşılacaktır. Bu amaçla, ikinci bölümde kısaca şifreleme içerikli dersleri alan öğrencilerin genel profili verilmiş, ardından üçüncü bölümde şifreleme ve güvenlik eğitiminde kullanılan yöntemler belirtilmiştir. Son olarak CrypTool ana başlığı altında, ilgili yazılım tanıtılmış, ders kapsamında eğitimde kullanılma biçimi ele alınmıştır.

2. Öğrenci Profili

Bilgisayar Mühendisliği Bölümü'nde, lisans ve lisansüstü eğitimlerde seçmeli olarak verilen şifreleme ve güvenlik dersleri, bu konulara merak duyan, giriş yapmak isteyen ya da güvenlik alanında uzmanlaşmayı amaçlayan öğrenciler tarafından tercih edilmektedir. Öğrenci sayısı, değişkenlik gösterebilmekle birlikte, diğer temel bilgisayar mühendisliği seçmeli derslerine göre daha düşük olmaktadır.

Lisansüstü derslerinde, gelecekte akademik kariyer yapmayı planlayan öğrenciler ile birlikte, özel sektörde tam zamanlı olarak yazılım ve bilişim alanında çalışan kişiler de bulunabilmektedir.

Dersi seçme amaçlarındaki olası farklılığa rağmen öğrenciler, belli bir matematik, teknik ve programlama eğitimi geçmişine sahip; bilgisayar ve elektrik-elektronik mühendisliği kökenli kişiler olarak ortaklık göstermektedir. Bu ortaklık, derslerin anlatımı ve uygulamalarda seviyeyi belirlemekte kolaylık sağlamaktadır.

3.Şifreleme ve Güvenlik Eğitiminde Kullanılan Yöntemler

Kriptografi eğitiminde, özellikle iletişim kurallarının anlatımında, görsel metaforlara ve araçlara başvurmak en çok kullanılan yöntemlerden birisidir. Bu metaforlara verilebilecek en önemli örnek, Alice-Bob, Ahmet-Belgin, gibi genel bir iletişim kanalı üzerinden iki sanal karakterin haberleşmesidir. Bu karakterler üzerinden öğretmen, sunu ya da tahta üzerinde sıralı gerçekleşen çeşitli iletişim kurallarının adımlarını ya da iletişimi tehdit eden unsurları gösterebilmektedir [6]. Şekil 1'de örnek olarak gösterilen tekrar (replay) atağında Bob, Alice'e bir mesaj göndermekte, bu mesajı dinleyen üçüncü kişi aynı mesajı Alice'e tekrar göndermektedir. Bu tür görsel araçların kullanımı kriptografi kavramlarının akılda kalıcılığını arttırmaktadır.

Şekil 1: Tekrar (replay) atak

Kullanılan diğer bir yöntem ise kriftografik algoritmaların ve iletişim kurallarının herhangi bir programlama dilinde kodlanmasına yönelik ödevlerin verilmesidir. Programlamaya yönelik daha kapsamlı projeler ile öğrenciler A, B, C gibi gruplanıp, A ve B grupları şifreli olarak haberleşmeye çalışırken, C grubundaki öğrencilerin bu haberleşmeyi çözmeye çalışmasıdır. Bu tür ödevler aracılığı ile öğrenciler algoritmaların içeriği ve uygulama biçimine dair pratik yapma olanağı bulabilmektedir [3].

Java applet, Flash veya benzeri hareketli görsel bilgisayar uygulamaları ile de kriptografinin anlatılması mümkündür. Buna yönelik olarak bazı uygulamalar bulunmakla birlikte, bunlar kullanıcının kendi ihtiyaçlarına göre değişiklik yapmasına olanak tanımamakta, sadece sundukları görsellikle konuların kavranmasına yardımcı olmaktadırlar [7].

Kriptografi eğitiminde kullanılmak üzere geliştirilmiş, hem görsellik barındırıp hem de kullanıcının ihtiyaçlarına göre değişiklik ya da ekleme yapabileceği uygulamalar içerisinde TECP [8], GRACE [6], CrypTool [9] sayılabilir.

Estonya Tartu Üniversitesi'nden Jelena Zaitseva, Jan Willemson ve Jaanus Pöial'ın Borland Kylix 3 Open Edition ve Borland Delphi 6 Personal Edition kullanarak geliştirdiği GPL lisanslı Tutorial Environment for Cryptographic Protocols (TECP) görsel ortamı genel anahtar şifreleme

öğretiminde kullanılmak üzere geliştirilmiş bir araçtır. Linux ve Windows işletim sistemine sahip bilgisayarlarda kullanılabilmektedir. Modüler aritmetiğe dayanan kriptografik protokollerin yaratılmasına ve işlenmesine olanak sağlar. Bu araç ile genel anahtar şifreleme protokolleri adım adım izlenerek yapılandırılandırılabilir. Ayrıca isteğe bağlı parametreler kullanılabilir ve iletişim grupları eklenebilir. Çok büyük tamsayılarla çalışılabilir. Ayrıca yapılandırılan protokoller saklanabilir [10].

TECP eğitim ortamında protokoller dizi diyagramları (sequence diagram) şeklinde gösterilmektedir. Bu yöntemle iletişim gruplarının ne zaman protokol adımlarına dahil olduklarının gösterilmesi amaçlanmıştır. TECP eğitim ortamının sunduğu iletişim grubu ekleme/silme, transfer edilen veriyi ekleme/değiştirme/silme, protokol değişkenini ekleme/değiştirme/silme gibi protokolü değiştirebilme imkanları, bu değişikliklerin protokol güvenliğini nasıl etkileyeceğini görmeye olanak sağlamaktadır[10].

Küçük gruplar ya da bireysel akademik çalışmaların ürünü olan TECP ve GRACE'in aksine, geniş katılımlı açık kaynak kodlu bir ortak proje olarak geliştirilen CrypTool, basit online uygulamalar [11], görsellik, kullanıcının kendi ihtiyaçlarına göre uyumlu eklenti geliştirebilmesi (CrypTool 2 [12]) gibi özellikleri ile eğitsel bir uygulama olarak öne çıkmaktadır.

4.CrypTool

4.1 CrypTool Nedir?

CrypTool; kriptografik algoritmaları uygulamak ve analiz etmekte kullanılmak üzere, Windows, Linux ve MacOS işletim sistemleri için geliştirilmiş bir e-öğrenme uygulamasıdır [9]. CrypTool projesi; çekirdek grubunu bilgisayar bilimleri ve matematik öğrencilerinin oluşturduğu farklı ülkelerde bulunan üniversitelerdeki ve şirketlerdeki insanlar tarafından geliştirilmiştir [9]. Projenin amacı, kullanıcılara kriptolojide kullanılan çeşitli kavramları ve teknikleri anlamada yardımcı olmaktır [2].

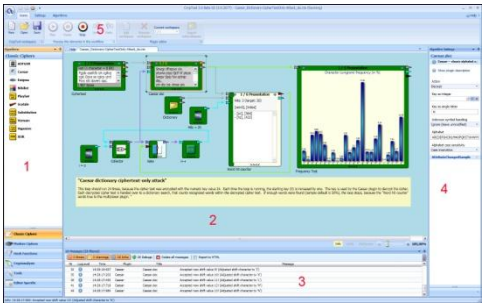
CrypTool projesi 1998 yılında başlamış, CrypTool 2000 yılında ücretsiz yazılım olarak kullanılmaya başlanmıştır. 2003 yılında ise CrypTool açık kaynak olarak dağıtılmaya başlanmıştır [9]. 2007'de CrypTool İngilizce, Almanca, Lehçe ve İspanyolca olarak hazırlanmıştır. 2008 yılında ise. NET ve Java sürümleri geliştirilmiştir. Şu an CrypTool'un 1.4.2.1 sürümü, JCrypTool Beta ve CrypTool 2 beta sürümleri mevcuttur. 1.4.2.1 sürümü C/C++ ile Visual Studio .NET 2003 ortamında geliştirilmiştir. JCrypTool sürümü Eclipse ortamında Java programlama dili ile, CrypTool 2 ise C# programlama dili ile Visual Studio 2008 ortamında geliştirilmektedir. CrypTool 2'nin geliştirilmesiyle birlikte CrypTool 1.x'in geliştirilmesi durdurulmuş, sadece yazılım hataları düzeltilmeye devam etmektedir.

Cryptool 2.0, Apache 2.0 lisansına sahiptir. Apache 2.0 lisansı, telif hakkı koruma ve feragat uyarısı gerektirmektedir. Apache 2.0 lisansı ile lisanslı uygulamaların kaynak kodları, özgür yazılım ve açık kaynak kodlu yazılımların geliştirilmesi için kullanılabilir. Fakat, Apache 2.0 lisansı copyleft lisanslarından farklı olarak, değiştirilmiş sürümlerin özgür ve açık kaynak kodlu yazılım şeklinde dağıtılma zorunluluğu getirmemiştir [13].

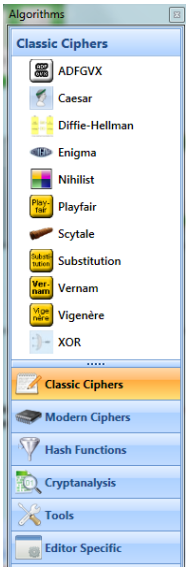
CrypTool 2 yazılımının sağladığı olanaklar şu şekilde listelenebilir:

- Ücretsiz bir yazılımdır.
- Kriptografik mekanizmaları aynı ortamda, uygulama, analiz etme ve öğrenme imkanı sağlar.
- Tipik Windows uygulaması ve görünümü olması (Şekil 2) anlaşılabilirliğini ve kullanılabilirliğini kolaylaştırır.
- Hem klasik hem modern şifreleme sistemlerini içerir.
- İçerdiği her şifreleme sistemiyle ilgili kısa

bir açıklama içerir ve çevrimiçi destek sağlar.
- Algoritma detaylarına girmeden sadece girdileri vererek çıktıları kolaylıkla elde edebilmenizi sağlar.
- Başlangıç için öğretici örnek projeler içerir [9].



Şekil 2: CrypTool 2 ana ekran görüntüsü



Şekil 3: Uyumlu Ek seçim penceresi

4.2 Uyumlu Ek (Plug in) Geliştirme

CrypTool 2 kurulumu, geliştirme ekibinin hazırladığı standart şifreleme (AES, DES, Enigma vb), analiz (frekans, Kasiski vb.) ve araçlar (metin girişi/çıkışı, karşılaştırma, sözlük vb) gibi ana başlıklar altında toplanmış uyumlu ekler (eklentiler) ile birlikte sunulmaktadır. Bu eklerin (Şekil 3) sürükle bırak mantığı ile proje ekranına taşınıp birbirlerine bağlanarak işlevlerini yerine getirmesi sağlanmaktadır (Şekil 4).

Kurulum ile gelen standart ekler, kullanıcının ihtiyaçlarını karşılamadığında ya da öğrencilerin algoritma ve iletişim kurallarını kendilerinin kodlamaları istendiğinde, CrypTool 2 ile uyumlu yeni ekler geliştirmek mümkündür.

CrypTool 2, .Net Framework üzerine kurulu "pure-plugin" (saf uyumlu ek) mimarisine sahip bir yazılım olduğundan, kişinin kendi eklentisini geliştirmesi için kısaca yeni eklentinin sınıfına (şifreleme, kriptanaliz, vb.) ait arayüzleri (interface methods) tanımlaması ve bu arayüzlerin içlerini doldurması yeterlidir.

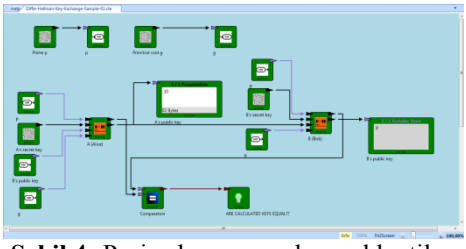
Bunun için takip edilecek adımlar şu şekilde özetlenebilir:

1. VisualStudio 2008'de yeni bir C# projesi yaratılır. Yaratılan projeye eklentiye uygun bir isim verilir (MD5, DES, vb.).
2. Projeye içerisinde gerekli arayüzlerin ve tanımlamaların olduğu "CrypPluginBase.dll" kütüphanesi referans olarak eklenir.
3. CrypTool 2'de her uyumlu ek için projede iki adet sınıfın bulunması gerekmektedir. Bunlardan birincisi eklentinin işlevini yerine getirecek olan "algoritma" sınıfı, diğeri ise (eğer varsa) kullanım esnasında eklentiye ait ayarların değiştirilmesini sağlayacak olan "ayarlar" sınıfıdır. Üçüncü adımda projeye bu iki sınıf eklenir (örn: DES.cs, ve DESSettings.cs).
Ardından bu iki sınıfın arayüzlerini miras alacakları isim uzayları (namespace) dahil edilir. Sınıfın yerine getireceği işleve göre CrypTool 2'de "Analysis", "Generator", "Cryptography" gibi isim uzayları ve bu isim uzaylarında da tanımlı sınıflar bulunmaktadır (örn: Hashing için IHash, şifreleme için IEncryptionAlgorithm, algoritma ayarları için IEncryptionAlgorithmSettings gibi).
4. CrypTool 2'de yaratılan eklentinin ayırt edilmesini sağlayacak PNG formatında bir ikon projeye eklenir.

5. Eklentinin diğer eklentiler ile bağlantısını sağlayacak giriş ve çıkış nesneleri "algoritma" sınıfına eklenir (örn: AES için giriş düz metin, anahtar; çıkış ise şifreli metin gibi).
Son olarak eklentinin işlevini yerine getirmesi için miras alınan arayüz metodlarının içerisinde eklentiden beklenen davranışa yönelik kodlama gerçekleştirilir (örn: AES veya herhangi bir şifreleme eklentisi için `Encrypt()`, `Decrypt()` gibi).

Kodlama tamamlandığında, oluşturulan proje derlenir ve elde edilen "dll" (Dynamic link library) dosyası CrypTool 2 kurulumunun "CrypPlugins" klasörü altına kopyalanır. Bir sonraki açılışta program yeni oluşturulan eklentiyi tanıyacak, ilgili başlık altına ekleyecektir (Şekil 3). Eğer eklenti ile ilgili bir problem varsa bu hata, programın açılış anındaki çıktılarından ya da açılış sonrası ilgili eklenti kullanılmak istendiğinde uygulama penceresinin "mesajlar" (Şekil 2) bölümünde oluşacak uyarılardan gözlenebilir.

Burada özet olarak ifade edilen eklenti hazırlama yöntemi, daha detaylı anlatımları ile [14] ve [15]'te bulunabilir.



Şekil 4: Proje ekranı ve çalışan eklentiler

Açık kaynak kodlu olan CrypTool 2'de eklenti geliştirmekte zorluk çekilmesi durumunda, İnternet üzerinden standart kurulum içerisinde bulunan tüm eklentilerin kaynak kodları incelenebilmekte, gerektiğinde bunlar örnek alınarak geliştirme yapılabilmektedir [16].

4.3 Derste Kullanımı ve Değerlendirmeler

Kriptografi içerikli dersler kapsamında, ilk aşamada CrypTool 2'nin mevcut kurulumu ile birlikte gelen eklentileri (Şekil 3) kullanılmış, bu eklentiler birbirlerine bağlanarak basit anlamda kriptografik algoritmaların çalışması gözlenmiştir (Şekil 4). Bu yolla öğrenciler uygulamanın yeteneklerini tanırken, aynı zamanda derste işlenen temel kriptografik algoritmaları görsel olarak deneme şansı bulmuşlardır.

İkinci aşamada öğrencilerden, iki girişini XOR ("dışlayan ya da", "exclusive or") işleminden geçirip çıkışına veren basit bir eklenti tasarlamaları istenmiş, bu basit uygulama ile öğrencilerin eklenti geliştirmeyi öğrenmeleri sağlanmıştır.

Son olarak öğrenciler, Diffie-Hellman anahtar değişimini gerçekleştirmeye yönelik bir eklenti geliştirmiş ve bu eklentinin kullanılışını hazırladıkları örnek CrypTool 2 projesi üzerinden göstermişlerdir.

CrypTool 2'nin bu üç aşamalı kullanımında birinci aşamada kayda değer bir zorluk ile karşılaşılmamış, uygulamanın kolay kullanımlı arayüzü ve görselliği, kriptografik algoritmaların tanınmasına katkı sağlamıştır.

İkinci aşamada ise talep edilen basit işlevine rağmen eklentiyi çalışır hale getirmek daha önce buna benzer bir çalışmayı yapmamış öğrenciler için zorlayıcı olmuştur. İlk eklentinin hazırlanması için geçen süre, öğrencilerin bildikleri bir programlama dilinde talep edilen işlevi yerine getiren bir kod yazmaları için geçen sürenin çok üzerinde olmuştur. Bununla birlikte, eklenti geliştirme süreci bir kere başarı ile tamamlandığında daha sonraki denemeler ve üçüncü aşamadaki ödev daha hızlı bir şekilde tamamlanabilmiştir.

Unutulmamalıdır ki birçok eklenti CrypTool 2 kurulumu ile hazır gelmektedir. Örneğin, kendi AES eklentisini hazırlayan bir kişinin

bu eklentiye "düz metin" girişi yapabilmek için kullanacağı metin "giriş" eklentisi, çıktıyı gözlemek ya da dosyaya yazdırmak için kullanacağı "çıktı" eklentileri, standart kurulum ile hazır gelmektedir. Kişinin, "yardımcı" olarak adlandırılabilecek bu eklentiler için ayrıca vakit kaybetmesine gerek kalmayacaktır.

CrypTool 2 henüz geliştirme aşamasında olduğundan çıkan yeni sürümleri ile eski sürümleri arasında eklenti uyumsuzluğu olabilmekte, bunu aşmak için problem görülen eklentiyi yeni sürümün kütüphanesi ile tekrar derlemek gerekebilmektedir.

5.Sonuç

Bilindiği gibi Kriptografi eğitiminde sorunların bir kısmı algoritmaların çok fazla matematiksel temelli ve karmaşık olmasıdır. Bir görsel aracın kullanımına ihtiyaç duyulmaktadır.

Görsel araç olarak seçilen Cryptool yazılımının 2. sürümü yardımıyla algoritmalar daha kalıcı bir şekilde öğrencilerde yer etmiştir. Yazılımın halen beta sürecinde olmasından dolayı karşılaşılan sorunlar haricinde önemli bir sorunla karşılaşılmamıştır. Gerektiğinde yeni algoritmalar ve protokoller de yazılıma eklenebilmiştir.

6. Kaynaklar

[1] Aboutabl, M.S., "The CyberDefense Laboratory: A Framework for Information Security Education", **Information Assurance Workshop, 2006 IEEE (1-4244-0130-5),** 21-23 June 55-60 (2006).

[2] Kendall J., "Cryptographic Techniques for Network Security using CrypTool", (University of Portsmouth, Project Report) April, 91 pages http://www.cryptool.org/ images/Project Jamie Kendall v1.1_final.pdf (2008).

[3] Temkin, A., "Teaching Cryptography to Continuing Education Students", **IFIP International Federation for Information Processing** 2007-10-27.Vol.237 121-128, (2007).

[4] Rocca, C. F., " Cryptology in General Education", **Cryptologia**, 29: 4, 337-342 (2005).

[5] Sakalli, M.T., Bulus, E., Buyuksaracoglu, F., "Cryptography Education for Students", **Information Technology Based Higher Education and Training, 2004**, 621-626 (2004).

[6] Cattaneo G., De Santis, A., Ferraro Petrillo, U., "Visualization of cryptographic protocols with GRACE", **Journal of Visual Languages and Computing,** April 2008, Vol.19, Iss.2; 258-290 (2008).

[7] Anane, R., Purohit, K.; Theodoropoulos, G.,. "An Animated Cryptographic Learning Object", **Computer Graphics, Imaging and Visualisation, 2008** 61-68 (2008).

[8] Zaitseva, J., "TECP—Tutorial Environment for Cryptographic Protocols", **Master's Thesis**, University of Tartu, (2003).

[9] CrypTool, http://www.cryptool.org, (2009).

[10] Zaitseva J., Willemson Jan, Pöial Jaanus, "TECP – Tutorial Environment for Cryptographic Protocols", University Of Tartu, (2003).

[11] CrypTool Online http://www.cryptool-online.org/, (2009).

[12] CrypTool 2 http://cryptool2.vs.uni-due.de (2009).

[13] Apache License Version 2.0, http://www.apache.org/licenses/LICENSE-2.0.html, (2009)

[14] Przybylski S., Wander M., "HowTo – Create a Hash-Plug-in for CrypTool 2",

http://cryptool2.vs.uni-due.de/downloads/howto/howto_hashplugin.pdf, (2009).

[15] Przybylski S., “HowTo – Create an Encryption-Plugin for CrypTool2.0”, http://cryptool2.vs.uni-ddue.de/downloads/howto/howto_encryptionplugin.pdf, (2009).

[16] CrypTool 2 Source Code Trunk https://www.cryptool.org/svn/CrypTool2/trunk/ (2009).