Linux Yaz Kamp 2015 "Kriptoloji ve Ters Kod Kursu":
PGP, Openssl ve Kriptografik kütüphane/yazılım kullanıma dair sorular

Eğitmen: Hamdi Murat Yıldırım (http://hmurat.bilkent.edu.tr)

1. İzleyen her işlemi gerçekleştirmek için hangi ilgili GnuPGP (gpg) komudunu çalıştırmak ve/veya hangi yolu izlemek gerekir?

   a) Hem dosya/e-posta imzalamak hem de şifrelemek için kişinin asimetrik açık/kapalı anahtar ikilisi yaratılması;

   b) Açık erişim anahtar sunucularına açık anahtarın aktarılması;

   c) Bir kişinin açık anahtarının b) şıkkında bahsi geçen sunucular üzerinde bulunması ve sistemdeki açık anahtarlığa aktarılması;

   d) Belirlenen herhangi bir dosyanın imzasının yaratılması;

   e) Arkadaşınız tarafından gönderilen dosya ve o dosyanın PGP imzasını kullanarak imza doğrulamanın gerçekleştirilmesi;

   f) Bir dosyanın simetrik şifreleme algoritması ile şifrelenmesi;

   g) f) şıkkındaki şifreli dosyanın deşifrelenmesi;

   h) a)-e) şıklarındaki işlemlerin (d) ve e) şıklarında e-posta mesajları düşünün) için Thunderbird yüklenecek eklenti Enigmail ile gerçekleştirilmesi

2.
   a) Bir arkadaşınıza thunderbird üzerinden Enigmail yardımıyla hem şifreli hemde imzalı e-posta mesajı gönderiniz.

   b) a) şıkkında hangi bilgi güvenliği hedefleri sağlanmıştır? Açıklayınız.

   c) a) şıkkında simetrik anahtar paylaşımı gerçekleşiyor mu? Cevabınızı açıklayınız.

3. Web ten imzası ile birlikte paylaşılan bir uygulama/programın dosyasını (Tor Browser -tarayıcı- veya GNU projesinden ilgili bir uygulama vb.) indiriniz ve bu imzayı doğrulamak için gerekli basamakları gerçekleştiriniz.

4. OpenSSL C kütüphanesi (JAVA üzerindne kullanımı mümkün) veya Bouncy Castle kütüphanesini veya benzeri özgür yazılım kütüphane/yazılım kullanarak izleyen işlemlerden bir veya birden fazlasını, grafik arayüze sahip veya komut satırından koşturulacak uygulamaları gerçekleştiriniz:

   a) Anahtar üretimi, verilen dosya şifreleme ve şifreli dosyanın deşifrelemesi (uygun simetrik şifreleme ve blok mod işlemleri (ECB, CBC, CTR vb. Kullanarak);

   b) Anahtar üretimi, verilen oldukça küçük dosya şifreleme ve şifreli dosyanın deşifrelemesi (Bazı asimetrik şifreleme algoritmaları kullanarak).

   c) Verilen dosyaların özet/parmak izi değerlerinin hesaplanması

5. Openssl komutları kullanarak kendinden (self-signed) imzalı SSL sertifikasıNI alan adınız veya lokal sisteminiz için oluşturunuz. Bu sertifikayı oluşturduktan sonra **https** bağlantısını sağlamak adına apache web sunucusu için gerekli ayarları yapınız. Bu işlemler sonucunda https bağlantısının yapılıp, yapılmadığını kontrol ediniz.

6. "The GNU Multiple Precision Arithmetic Library (gmp)" kullanarak

   a) çok büyük tam sayılar için (512, 1024, 2048-bit vb.) çarpma, toplama, modüler aritmetik ve üst alma işlemlerini gerçekleştiren örnek C dili kodlarını yazınız.

   b) örnek bir C dili kodunu çok büyük asal sayılar oluşturmak için yazınız.

7. İzleyenler kütüphanelerden birini kullanarak

   - Bouncy Castle C# or Java APIs
   - GNU Libgcrypt
   - cryptlib
   - phpcrypt: A PHP Encryption Library API which does not use 3rd party libraries

   izleyen işlemleri gerçekleştiren programlama dili kodlarını yazınız:

   i. Simetrik şifreleme: dosya şifreleme/deşifrelemesi için

   ii. Özet fonksiyonlar: özet/parmak izi yaratma için

   iii. Asimetrik şifreleme: anahtar paylaşımı ve dijital imzalama için

   iv. HMAC: mesaj kimlik doğrulama için