TOBB-ETÜ, MATEMATİK BÖLÜMÜ, 2014-2015 BAHAR DÖNEMİ
MAT 421/515, ŞİFRELEME BİLİMİNE GİRİŞ/KRİPTOLOJİ I, FİNAL SINAVI
8 NİSAN 2015

Adı Soyadı:
No:
İMZA:

1) $\begin{cases} e = 65537 \\ p = 2147483659 \end{cases}$ olmak üzere $ed = 1 \bmod p$ eşitliğini sağlayan d değerini hesaplayınız.

2) Bir sınıfta en az iki kişinin aynı doğumgününe sahip olma olasılığının %50'den fazla olması için sınıf mevcudu en az kaç olmalıdır?

3) Aşağıdaki kriptografik algoritmalardan hangisi şifreleme yöntemi değildir? Nedenini açıklayınız.

A) Keccak B) AES C) RSA D) A5/1 E) Caesar

4) Açık anahtarlı kriptosistemlerden birisi olan RSA algoritmasının güvenliği matematiksel olarak hangi probleme dayanmaktadır?

5) Açık anahtarlı şifreleme algoritması kullanan bir kullanıcı kaç anahtara sahiptir? Nedenini açıklayınız.

6) $128-$bit uzunluğunda bir şifreleme algoritması anahtarı için tüm ihtimalleri deneyerek doğru anahtarı bulmak istiyoruz. Denemeyi yapacak her işlemci çekirdeğinin saniyede 2^{48} deneme yaptığını varsayalım. Dünya üzerindeki toplam insan sayısını 2^{33} (yaklaşık 7 milyar) kabul edelim. Her insanın $1024 (= 2^{10})$ çekirdekli işlemcilere sahip bilgisayarlarının olduğunu varsayalım.

Bu durumda tüm ihtimalleri denemek yaklaşık 2^n saniye sürecektir.

n değerini hesaplayınız.

7) Simetrik şifreleme için DES (Data Encryption Standard) blok şifrelemesini 56-bit anahtar uzunluğu ile 896-bit büyüklüğünde bir dosyayı şifrelemek için kullandığımızı varsayalım. Bu işlem için toplamda kaç tane DES şifrelemesi yapmamız gerekir?

8) Türkiye'de hangi kurum/kurumlar Nitelikli Elektronik Sertifika Hizmet Sağlayıcısıdır?

9) Ülkemizde kullanılan Nitelikli Elektronik İmza hizmeti için en son yayınlanan tebliğ doğrultusunda imza sahibi tarafından DSA algoritmasının kullanılarak imza oluşturma veya doğrulama işlemlerinde en az kaç bit anahtar kullanılması gerekmektedir?

10) Aşağıdakilerden hangisi bağlandığınız web siteleri ile aranızdaki iletişimin güvenli olmasını sağlayan kriptografik protokollerden birisidir? Nedenini açıklayınız.

A) TLS B) PGP C) XTR D) LLL E) SMS

11) Temel güvenlik hedeflerini ve bu hedeflere ulaşmak için kullanılabilecek algoritmaların isimlerini yazınız.

12) Kullanıcı C, e-posta iletimine müdahale edebilir ve bu dosyayı başka bir dosya ile değiştirip, sanki mesaj Kullanıcı A dan geliyormuşcasına tekrar Kullanıcı B ye gönderebilir. Bu durumun gerçekleşmesiyle hangi güvenlik hedefi ihlal edilmiş olur?

13) Kullanıcı C'nin, Kullanıcı A yerine, bu kullanıcıdan gönderiliyor izlenimi verilerek (Kullanıcı A böylesine bir mesajı Kullanıcı B'ye göndermemektedir), Kullanıcı B'ye e-posta mesajı göndermesi durumunda hangi güvenlik hedefi ihlal edilmiş olur?

14) Müşteri B, çağrı merkezi üzerinden müşteri temsilcisi G'ye bir talimat vermiştir ve G bu talimatı yerine getirmemiştir. B, durumu anlaması üzerine yetkililer ile görüşmüş ve G de bu talimatı aldığını inkar etmiştir. Bu durumda G hangi güvenlik hedefinin eksikliğinden faydalanarak bunu söyleyebilmiştir?

15) Bilgiyi gizlemek için şifrelemek yerine bilginin varlığını gizlemeye çalışan bilim dalı hangisidir?

16) **6B80D9DDAE26D7AC6F5D074E9E7BED119ED3D556**
Yukarıda hexadecimal olarak değeri verilen özet (hash) fonksiyon çıktısı aşağıdaki algoritmalardan hangisine aittir? Nedenini açıklayınız.

A) MD5 B) SHA1 C) SHA256 D) Keccak E) Whirlpool

17) A = 27e53c01aae41f764c2009fd17193327
B = 6aa06854e9b64626186f4eaf56497b7e

hexadecimal değerler olmak üzere **A XOR B** değerini hesaplayınız. Hesapladığınız değerin ASCII karşılığını bulunuz.

A XOR B = ?
ASCII = ?

18) 105 sayısının asal çarpanları 3, 5 ve 7 dir. Buna göre 601377231137 sayısının asal çarpanlarını bulunuz.

19) Aşağıdaki ağ iletişim protokollerinden hangilerinin kriptografik yöntemler ile güçlendirilmiş güvenli sürümleri standart olarak mevcuttur? Nedenini açıklayınız.

A) HTTP B) SMTP C) DNS D) ARP E) FTP

20)

$$a^n + b^n = c^n$$

a, b ve c sıfırdan büyük tam sayılar olmak üzere, n değerinin ikiden büyük ve tam sayı olduğu durumlarda yukarıdaki eşitliğin sağlanamayacağını gösteriniz.