Bilgi Güvenliği ve Kriptografi

Genel Anahtar Kriptosistemler

- Genel anahtar sistemlerde, şifreleme ve deşifreleme için kullanılan anahtarlar farklıdır.

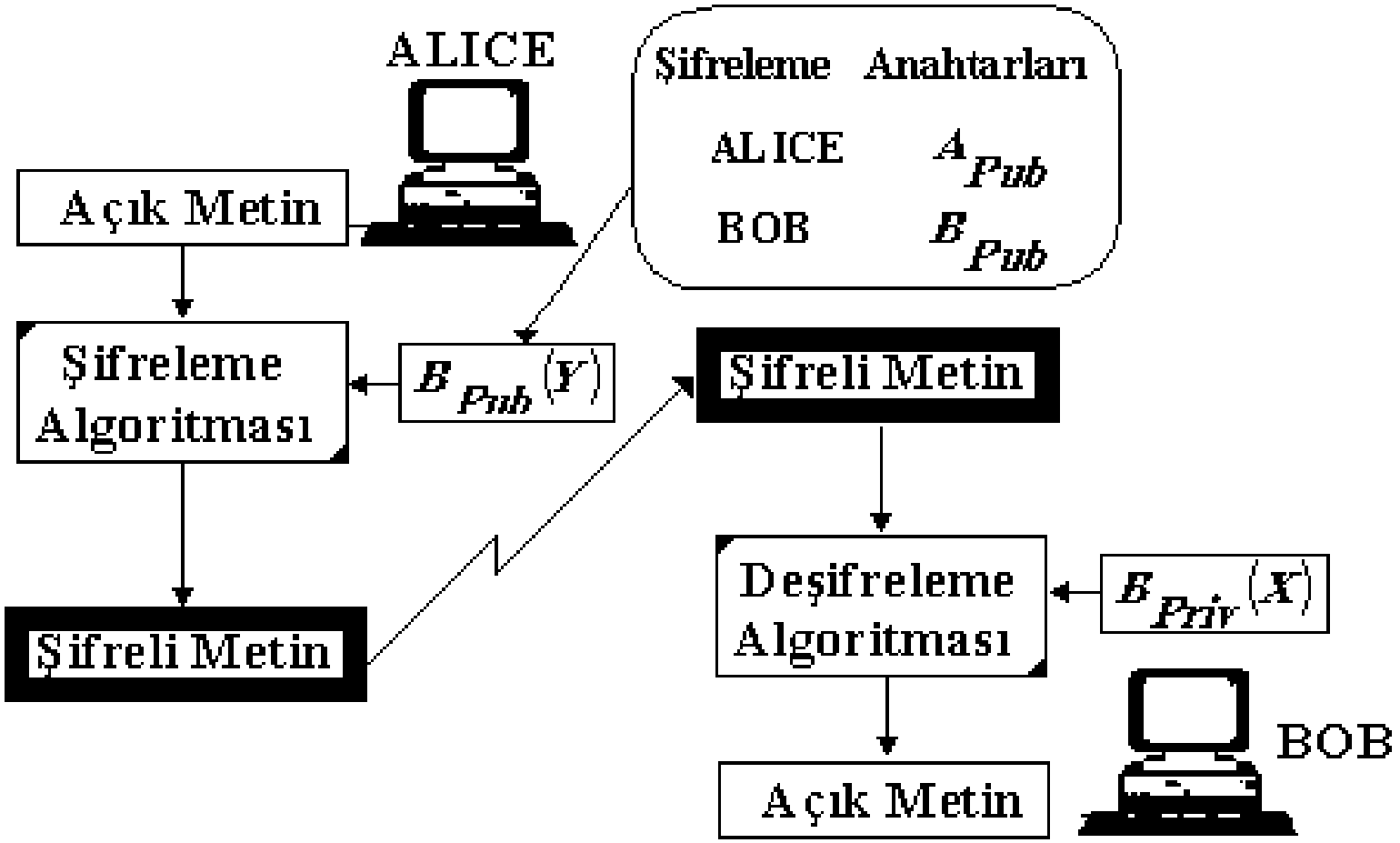
- Sistemdeki kişilerin genel anahtarları, herkesin erişebileceği bir veri tabanında tutulur.

Genel Anahtar Kriptosistemler

Genel anahtar kriptosistemde,

- Alice ve Bob bir kriptosistem üzerinde görüş birliğine varır.
- Bob Alice'e genel anahtarını gönderir.
- Alice mesajını Bob'un genel anahtarını kullanarak şifreler ve Bob'a gönderir.
- Bob özel anahtarını kullanarak mesajı deşifre eder.

Genel Anahtar Kriptosistemler



Genel Anahtar Kriptosistemler

- Burada önemli olan, şifrelemede kullanılan anahtardan, deşifreleme anahtarının elde edilmesinin çok zor olması gerektiğidir.

- Aksi halde, alıcı dışındaki kişilerin de şifreli mesajları deşifre edip okuması mümkün olacaktır.

- Çoğu uygulamalarda genel anahtar kriptografi *oturum anahtarının* (session key) gizli tutulması ve dağıtılmasında kullanılır. Daha sonra bu oturum anahtarı, bir simetrik algoritma ile birlikte kullanılarak mesaj trafiği gizlenir. Bu sisteme *hibrid* (hybrid) *kriptosistem* adı verilir.

Genel Anahtar Kriptosistemler

Bu sistem için haberleşme protokolü aşağıdaki aşamalardan oluşmaktadır.

- Bob Alice'e genel anahtarını gönderir.
- Alice rasgele bir *K* oturum anahtarını üretir ve bu anahtarı Bob'un genel anahtarı ile şifreleyerek Bob'a gönderir.

$$E_{B\_Public}(K)$$

- Bob Alice'in mesajını özel anahtarını kullanarak deşifre eder ve *K* oturum anahtarını elde eder.

$$D_{B\_Private}(E_{B\_Public}(K))=K$$

- Her ikisi de mesajlarını aynı oturum anahtarını ve simetrik bir yöntem kullanarak şifreler ve gönderir.

RSA Genel Anahtar Kriptosistemi

- RSA (R. Rivest, A. Shamir, L. Adleman) en çok kullanılan genel anahtar kriptosistemidir.
- RSA hem güvenlik, hem de sayısal imza için kullanılabilir.
- RSA'nın güvenliği çarpanlara ayırma probleminin zorluğuna dayanır.
- RSA ile yapılacak şifrelemede öncelikle anahtar üretimi yapılmalıdır.

RSA Anahtar Üretimi

- Aynı boyutlu p ve q gibi, iki büyük asal sayı üretilir. Büyüğün buradaki anlamı asal sayıların yüzlerce haneli sayılar olmasıdır. Bu sayede $p*q$ sayısının çarpanlarına ayrılması çok zor olacaktır. Bu da şifreleme sisteminin güvenliğini oluşturur.

- $n=p*q$ ve $\phi=(p-1) * (q-1)$ çarpımları hesaplanır.

- $1<e<\phi$ aralığında rasgele bir e sayısı $gcd(e,\phi)=1$ şartını sağlayacak şekilde seçilir. gcd fonksiyonu iki sayı için en büyük ortak böleni bulur.

- $1<d<\phi$ aralığında $ed \equiv 1 \pmod{\phi}$ şartını sağlayan d sayısı hesaplanır.

- Genel anahtar (n,e); özel anahtar ise d'dir.

RSA Genel Anahtar Şifreleme

- Mesajın gönderileceği kişinin genel anahtarı (*n*,e) elde edilir.
- Şifrelenecek mesaj, [0,*n*-1] aralığındaki bir *m* sayısına dönüştürülür.
- $c = m^e \bmod n$ hesaplanır.
- Oluşturulan *c* şifreli mesajı alıcıya gönderilir.

RSA Genel Anahtar Deşifreleme

- *d* özel anahtarı ile

$$m = c^d \bmod n$$

hesaplanır ve orijinal mesaj (m) elde edilir

RSA Şifreleme: Örnek

- Şifreleme yapılmadan önce anahtar üretimi gerçekleştirilmelidir.
- p=3, q=37 olarak seçilirse, n=3x37=111 ve ϕ=2x36=72 olarak hesaplanır.
- e=5 olarak seçilirse, d=29 olur. Çünkü 5x29≡1 (mod 72)'dir.

  Genel anahtar 111 ve 5

  Özel anahtar 29

RSA Şifreleme : Örnek

- Anahtar üretimi yapıldıktan sonra şifreleme işlemi gerçekleştirilir.
- Şifrelenecek mesaj, diğer adıyla açık metin "*y*>0" olsun.
- RSA'da işlemler sayılar üzerinden yapıldığından, mesaj sayısal bir ifadeye dönüştürülmelidir.
- Bu amaçla her karakterin ASCII kodu kullanılır. Bu durumda açık metin aşağıdaki şekli alır.

  y→121, >→062, 0→048 ⇒ "121062048"

RSA Şifreleme : Örnek

- Şifrelenecek sayılar *n*'den küçük olmak zorundadır. Bu nedenle sayısal metin *n*'nin basamak sayısının bir eksiği uzunluktaki parçalara ayrılır. Bu sayı L_{clear} olarak adlandırılır. Örnekte *n* sayısı 3 basamaklı olduğundan, L_{clear}=2 olur ve mesaj ikili bloklara ayrılır.

"12 10 62 04 8"

- Her blok L_{clear} basamaklı olmak zorundadır. Bu nedenle eksik kalan blokların sonuna gereken sayıda 0 eklenir.

"12 10 62 04 80"

RSA Şifreleme : Örnek

- Şimdiki aşama bu sayıların kurala uygun bir şekilde şifrelenmesidir. Şifreleme işlemi aşağıdaki şekilde yapılır.

$$12^5 \bmod 111 = 81$$
$$10^5 \bmod 111 = 100$$
$$62^5 \bmod 111 = 104$$
$$4^5 \bmod 111 = 25$$
$$80^5 \bmod 111 = 80$$

- Bu aşamada oluşan sayılar *n* ile aynı basamak sayısına sahip olmalıdır. Bu sayı L_{cipher} ile gösterilir. Örnek için L_{cipher} 3'e eşittir. Bu nedenle gerekli bloklar için sayıların sol tarafına gerekli sayıda 0 eklenmelidir. Bu durumda şifreli metin aşağıdaki hale gelir ve gönderilir .

"081 100 104 025 080"

- **Şifreli metin:** "081100104025080"

RSA Şifreleme : Örnek

- Deşifrelemede , alınan "081100104025080" şifreli metni öncelikle L_{cipher} uzunluklu bloklara bölünür ve hemen ardından deşifreleme kuralı uygulanır.

"081 100 104 025 080"

$81^{29} \bmod 111 = 12$

$100^{29} \bmod 111 = 10$

$104^{29} \bmod 111 = 62$

$25^{29} \bmod 111 = 4$

$80^{29} \bmod 111 = 80$

- Sonuçların L_{clear} uzunlukta olması gerekir. Bu nedenle uzunluğu L_{clear}'dan küçük olan blokların sol tarafına gereken sayıda 0 eklenir.

"12 10 62 04 80"

RSA Şifreleme : Örnek

- Son aşama, bu sayıların birleştirilmesi ve üçlü bloklara bölünmesi ile ASCII kodların elde edilmesidir. Fazlalık olarak oluşan 0'lar göz önüne alınmaz.

"1210620480"

"121 062 048"

121 → *y*, 062 → >, 048 → 0

- Sonuçta açık metin "*y*>0" olarak elde edilmiştir.