BİLGİSAYAR ve BİLİŞİM BİLİMLERİ FAKÜLTESİ

BİLGİSAYAR MÜHENDİSLİĞİ

KRİPTOLOJİYE GİRİŞ DERSİ
PROJE ÖDEVİ

KONU: RC4 Algoritması

İSİM : ABDULKADİR ABUŞ
NO : B151210111
GRUP : 1A

İSİM : ENES ZEREN
NO : B161210100

GRUP : 1A

1. **Genel Bilgi**

Ronald Rivest tarafından geliştirilen RC4 Şifreleme Algoritması, RSA , paylaşılan anahtarın güvenli alışverişini gerektiren bir paylaşılan anahtar akış şifresi algoritmasıdır.

RC4 artık güvenli sayılmamaktadır ve kullanımı ile ilgili olarak dikkatli bir şekilde düşünülmelidir.

Algoritma, anahtar dizisine dayalı olarak durum girişlerinin birbirini izleyen değişimlerini gerektirdiği için seridir. Bu nedenle, uygulamalar çok hesaplama olabilir. RC4 şifreleme algoritması, 40 ve 128 bit anahtarlar kullanılarak WEP (Kablosuz Şifreleme Protokolü) içinde IEEE 802.11 gibi standartlar tarafından kullanılır. WEP'de uygulanan güvenlik önlemlerinin kırılması için yayınlanmış prosedürler bulunmaktadır. Anahtar akışı kullanılan düz metinden tamamen bağımsızdır. Girişlerin her birinin 0 ile 255 arasındaki sayıların bir permütasyon olduğu ve permütasyonun değişken uzunluk anahtarının bir fonksiyonudur. Her ikisi de algoritmada kullanılan iki sayaç i ve j'dir.

Algoritma, 256 baytlık bir durum tablosunu başlatmak için 1 ile 256 bayt arasında bir değişken uzunluk anahtarı kullanır. Rasgele bayt üretimi için kullanılır ve daha sonra şifreli metin vermek için düz metin ile rastgele akış oluşturmak için kullanılır. Durum tablosundaki her öğe en az bir kez değiştirilir. Anahtar genellikle 40 bit ile sınırlıdır, ancak bazen 128 bit anahtar olarak kullanılır. 1 ile 2048 bit arasında anahtar kullanabilme özelliğine sahiptir. RC4, Lotus Notes ve Oracle Secure SQL gibi birçok ticari yazılım paketinde kullanılmaktadır.

2. **Aşamalar**

Algoritma iki aşamada çalışır, anahtar kurulum ve şifreleme. Anahtar kurulum, bu şifreleme algoritmasının ilk ve en zor aşamasıdır. Bir N bit anahtar kurulumu sırasında, şifreleme anahtarı iki diziyi, durumu ve anahtarı ve karıştırma işlemi sayısını kullanarak bir şifreleme değişkenini oluşturmak için

kullanılır. Bu karıştırma işlemleri, takas bayt, modulo işlemleri ve diğer formüller içerir. Bir modulo operasyonu, bölümden kalan bir geri dönüşü sağlama işlemidir.

3. **Güçlü Yönleri**

- Herhangi bir değerin tabloda nerede olduğunu bilmenin zorluğu.
- Tablodaki hangi konumun, dizideki her bir değeri seçmek için kullanıldığını bilmenin zorluğu.
- Şifreleme, DES'den yaklaşık 10 kat daha hızlıdır.

4. **Zayıf Yönleri**

- RC4 artık güvenli kabul edilmiyor.
- Her 256 anahtardan bir tanesi zayıf bir anahtar olabilir. Bu anahtarlar, kriptanaliz tarafından bulabilmektedir.
- Belirli bir RC4 Algoritması anahtarı sadece bir kez kullanılabilir.

5. **Performans**

UDI uygulamalarının her biri, uygulama için özel olarak tasarlanmış bir donanım bloğudur. Anahtar alan için durum tablosunu yerel olarak sürdürmek için anahtar bayt jeneratörü tarafından RAM alanı gereklidir. Diğer süreçlerin aynı işlevselliğe ihtiyaç duyacağı durumlarda, bir bağlam değişikliği durumunda bu durumun korunması ve geri yüklenmesi gerekecektir. Bu performans, yukarıdaki performans projeksiyonlarında dikkate alınmamıştır. Şifreleme ve şifre çözme durum verileri, bağımsız süreçlere izin vermek için ayrı durum belleklerinde depolanabilir.

6. Ekran Çıktısı