İkame Kutusu

Kriptografide bir S-Box, ikameyi gerçekleştiren simetrik anahtar algoritmasının temel bir bileşenidir.

Blok şifrede, genellikle anahtar ve şifreli metin-Shannon'ın karışıklık özelliği arasındaki ilişkiyi gizlemek için kullanılırlar.

Genel olarak, bir S-Box 'm' girdi bitlerini alır ve bunları 'n' çıkış bitlerine dönüştürür, burada 'n' mutlaka 'm' ile eşit değildir.

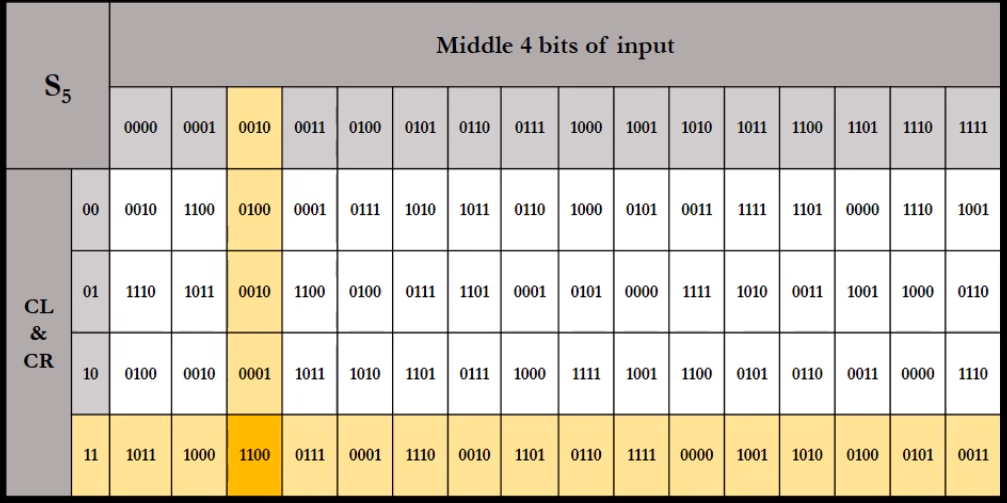
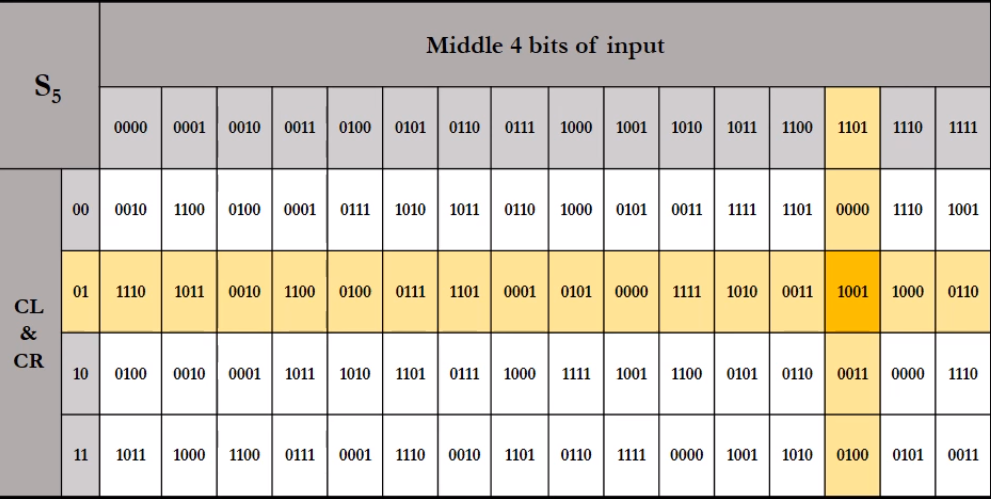
Bu bir m \* n S-Box olarak adlandırılır ve genellikle bir arama tablosu olarak uygulanır

Veri Şifreleme Standardı'nda (DES) olduğu gibi sabit tablolar normal olarak kullanılır, ancak bazı şifrelerde tablolar dinamik olarak anahtardan oluşturulur

Bir sabitin iyi bir örneği DES'den (S5) gelen S-Box'tır, 6-bit girişini 4-bit bir çıkışa eşler

6-bitlik bir giriş verildiğinde, 4 bitlik çıktı, outher iki bit (CL & CR) ve iç dört bitleri kullanan sütun kullanılarak satırın seçilmesiyle bulunur.

***örneğin***, bir giriş (100101), çıkış bitlerine (11) ve iç bitlere (0010) sahiptir, karşılık gelen çıktı (1100) olacaktır.



DES'in 8 S-Box'ları, uzun yıllar boyunca, sadece tasarımcılarına ait bir arka kapı - bir güvenlik açığının, şifreye yerleştirildiği endişesiyle, yoğun bir çalışmanın konusuydu.

s-box tasarım kriterleri, diferansiyel kriptanalizin yeniden keşfedilmesinin ardından, bu özel saldırıya karşı direnci arttırmak için dikkatle ayarlanmış olduklarını gösterdikten sonra nihayet yayınlandı (1994 yılında).

Biham ve Shamir, S-Box'taki küçük değişikliklerin bile DES'i önemli ölçüde zayıflatabileceğini keşfetti.

özellikleri: her kontrol biti seçimi için, her çıktı biti, giriş bitlerinin doğrusal olmayan bir işlevidir.

S-Box'ın her satırı 4 doğrusal olmayan Boole fonksiyonundan oluşur. Bu doğrusal olmayanlık, DES için gerekli karışıklığın temelidir

S-Box'a tek bir giriş bitini zincirleme S-Box'ın en az iki çıkış biti

Bu, giriş bitlerinin istatistiksel özelliklerinin çıkış bitleri-difüzyonu üzerinde sperad olduğu anlamına gelir

Tek bir giriş biti sabit tutulduğunda, kalan 5 giriş biti değiştikçe, 2 ^ 5 = 32 çıkış yarı baytında 0'lar ve 1'ler arasında iyi bir denge vardır.

Bu, algoritma çıktısının tek bir dağılımını sağlar ve kriptanalistlerin istatistiksel çıkarımlar yapmasını engeller.