Homework-3

Mustafa Tokat

January 5, 2021

1 Introduction

bla bla

2 Analysis of Problems

2.1 Problem 1

...

2.2 Problem 2

2.2.1

(1)Suppose that $K_1 = K_2 = \cdots = K_{16}$. Show that all bits in C_1 are equal and all bits in D_1 are equal
(2)Show that there are exactly 4 DES keys for which all round keys are the same. They are called weak DES keys. Key Scheduling ciphertext üretiminden tamamen bağımsız bir süreçtir. Burada 56 bitlik anahtarın ilk yarısı left, ikinci yaısı right olrak adlandırılır. Ve bu sürecin tamamı logictir ve inverse edilebilir. Kısa çıklamanın ardından Ci ve Di lerin eşit olmasının arkasındaki mantıksal bağı kurabiliriz. Ki değerleri Ci ve Di değerlerinin kendi içlerinde lefthift işlemindensonra yanyana gelmesinden oluşmaktadır. Varsayımımıza göre bütün anahtarlarımız eşitse,bu aynı zamanda bütün Ci lerin eşit olduğu ve bütün Di lerin de eşit olduğu anlamına gelir.

Dikkatlice key schedulıng şemasını incelersek drop bazı bitleri drop edilmiş 48 bitlik PC_2 permutastyonun ilk yarısı 1-28 bitlerden ikini yarısın da 29-48. bitlerden oluştuğunu görebiliriz. Dolayısıyla PC_2 den çıkan Ki lerin ilk 24 biti left(Ci), ikinci 24 bitinin ise right(Di) bitleri oluşturduğunu rahatlıkl söyleyebiliriz. Aşağıdaki tablo açık olarak gösterecektir.

2.2.2

(3)Determine these 4 weak DES keys. Bu değerler NIST tarafından yayınlanmış olan blabla sayısında açıklanmıştır. Ve aşağıaki gibidir.
a = ...

2.3 Problem 3

2.4 Problem 4

Consider the AES/Rijndael algorithm and its Galois field GF(2^8)

2.4.1 Compute the sum (a7) + (5c) in GF(2^8)

dedede

2.4.2 Compute the product (a7) × (5c) in GF(2^8)

dedede

2.4.3 Compute S(a7)

dedede

2.4.4 Compute S^{-1}(5c)

dedede

2.5 Problem 5

deded