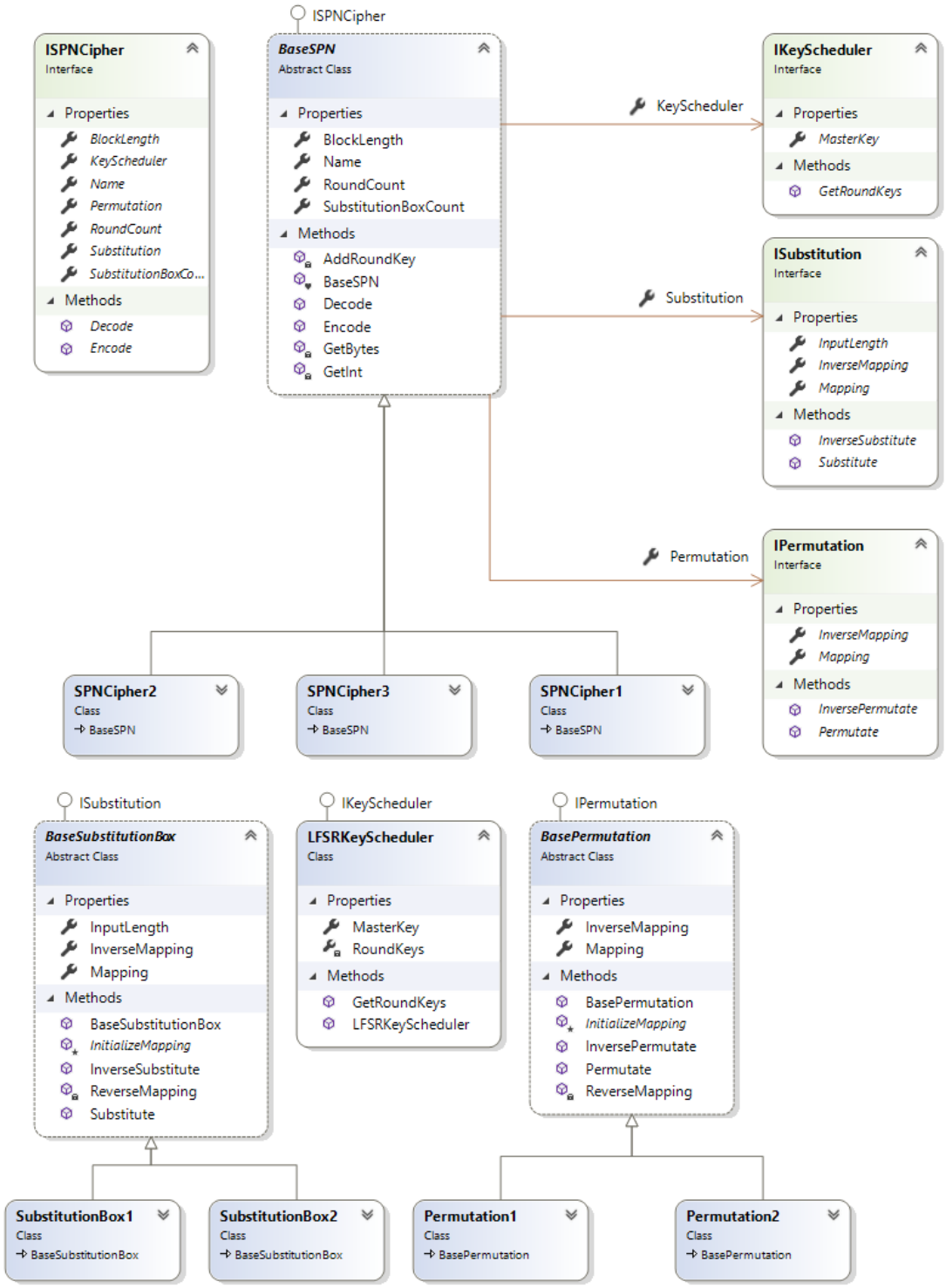
Yasin ÖZTÜRK 704171007

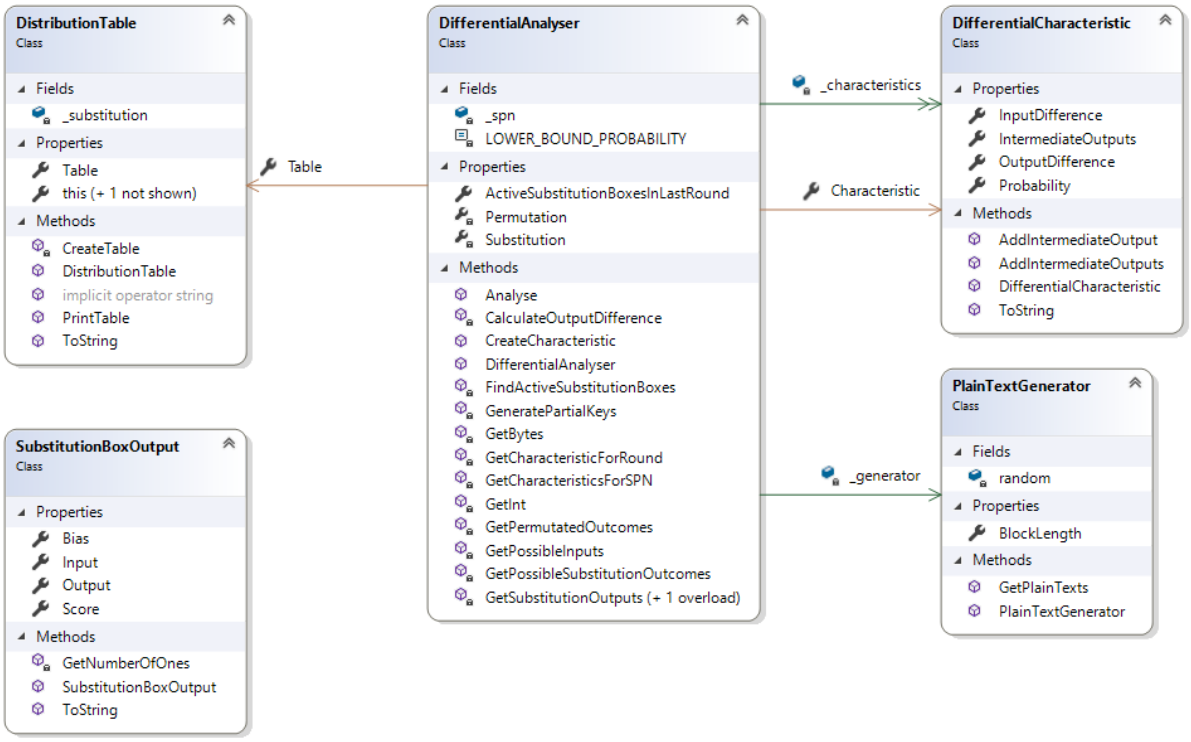
BLG520E Cryptography

2nd Homework

Verilen block cipher'ları kullanabilmek adına SPN Cipher'ın genel implementasyonu yapılmıştır. Aşağıdaki sınıf diyagramı, geliştirilen SPN Cipher framework'unun mimarisini göstermektedir.



Verilen block cipher'lara differential cryptanalysis uygulamak üzere DifferentialAnalyser adında bir sınıf geliştirilmiştir. Geliştirilen bu sınıf, block cipherların Difference Distribution tablolarını oluşturup, seçilebilecek tüm diferansiyel karakteristiklerini oluşturmaktadır. Tüm diferansiyel karakteristikler bulunduktan sonra, bu karakterteristikler içerisinde en büyük ihtimale sahip olan karakteristik seçilmektedir. Karakteristik seçildikten sonra, karakteristiğin ihtimaline göre yeterli miktarda plaintext-ciphertext çifti oluşturulmaktadır. Karakteristiğin belirlediği plaintext farkına göre oluşturulan rasgele çiftlerin ciphertextleri, cryptanalysis için tüm olabilecek son round anahtarları ile teker teker çözülmüş ve son round'un substitution kutularının çıkışına getirilmiştir. Bu kutuların çıkışları, substitution kutularının belirlediği eşleştirmeye göre girişe çevrilmiştir. Bu kısımda, bulunan diferansiyel karakteristiğin çıkışı ile, son round'daki substitution kutularının girişine getirilen ciphetextin farklarının eşit olup olmadığı kontrol edilmiştir. Diferansiyel karakteristik ile çözülen ciphertextin farkının aynı olması durumunda, denenen partial key'in görülme sayısı 1 arttırılmıştır. Aşağıda bu işlemleri gerçekleştiren DifferentialCryptanalysis framework'unun yazılım mimarisi verilmiştir.



Block cipher'larda şifrelemede kullanmak adına anahtar 31327 olarak seçilmiştir. Aşağıda, seçilen anahtarın LFSR Key Scheduling algoritmasına göre round subkey'leri verilmiştir.

- K_0 : 31327 ➔ 0111 1010 0101 1111
- K_1 : 48431 ➔ 1011 1101 0010 1111
- K_2 : 56983 ➔ 1101 1110 1001 0111
- K_3 : 61259 ➔ 1110 1111 0100 1011
- K_4 : 63397 ➔ 1111 0111 1010 0101
- K_5 : 64466 ➔ 1111 1011 1101 0010

Block cipher'lara sırasıyla differential cryptanalysis uygulandığında, aşağıdaki sonuçlar elde edilmiştir.

BLOCK CIPHER 1

Aşağıdaki resimde, geliştirilen programın çıktısı verilmiştir. Geliştirilen DifferentialAnalysis framework'u, Difference Distribution tablosunu oluşturup, resimdeki gibi tablo halinde yazdırmaktadır. Oluşturulan tablo yardımıyla, olabileck tüm giriş farkları denenerek diferansiyel karakteristikler oluşturulmuştur. Block Cipher 1 için bulunan en yüksek ihtimal sahip diferansiyel karakteristik, giriş farkının 1 olup çıkış farkının 2176 olduğu zaman gerçekleşmektedir. Her round'un giriş ve çıkış bilgileri aşağıdaki gibidir:

ΔU_1 : 1 ➔ 0000 0000 0000 0001
ΔV_1 : 4 ➔ 0000 0000 0000 0100 $\epsilon_1 = 4 / 16 = 0.25$
ΔU_2 : 256 ➔ 0000 0001 0000 0000
ΔV_2 : 2048 ➔ 0000 1000 0000 0000 $\epsilon_1 = 4 / 16 = 0.25$
ΔU_3 : 16384 ➔ 0100 0000 0000 0000
ΔV_3 : 24576 ➔ 0110 0000 0000 0000 $\epsilon_1 = 6 / 16 = 0.375$
ΔU_4 : 2176 ➔ 0000 1000 1000 0000

$\pi\epsilon = 0.25 \times 0.25 \times 0.375 = 0.0234375$
Plaintext-ciphertext çift sayısı = 20 / 0.0234375 ≈ 854

```
DIFFERENTIAL ANALYSIS OF SPN BLOCK CİPHER 1

Differential Table of SPN Block Cipher 1
   0   1   2   3   4   5   6   7   8   9   A   B   C   D   E   F
 ____________________________________________________________________
0 |  16  0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
1 |  0   0   0   0   4   0   0   0   4   0   2   2   0   0   2   2
2 |  0   0   2   0   2   0   2   2   0   0   0   2   6   0   0   0
3 |  0   0   2   2   2   0   2   0   4   0   0   0   2   0   0   2
4 |  0   0   2   2   0   0   6   2   0   0   4   0   0   0   0   0
5 |  0   0   4   0   0   0   0   0   4   4   0   0   0   0   4   0
6 |  0   4   0   0   2   0   2   0   0   0   4   0   2   0   2   0
7 |  0   0   2   0   2   4   0   0   0   0   2   0   2   0   4   0
8 |  0   0   0   4   0   2   0   2   4   0   0   0   0   2   0   2
9 |  0   0   0   2   0   2   0   4   0   0   0   2   4   2   0   0
A |  0   4   0   4   4   0   0   0   0   0   0   0   0   0   0   4
B |  0   0   0   0   0   0   0   4   0   0   2   6   0   0   2   2
C |  0   0   2   0   0   6   0   0   0   0   0   2   0   2   2   2
D |  0   4   0   0   0   2   2   0   0   0   2   2   0   2   0   2
E |  0   0   2   2   0   0   2   2   0   8   0   0   0   0   0   0
F |  0   4   0   0   0   0   0   0   0   4   0   0   0   8   0   0

Found Differential Expression:
1 X 2176 ==> 0,0234375

Found Partial Key:
0000 1011 1101 0000

DIFFERENTIAL ANALYSIS OF SPN BLOCK CİPHER 1 HAS COMPLETED
```

Bulunan diferansiyel karakteristik toplamda 3 adet subtitution kutusunu aktif hale getirmektedir ve son round'da da 2 adet substitution kutusuna giriş olarak bağlanmaktadır. Diferansiyel karakteristiğin ihtimali 0.0234375 olarak bulunmuştur ve yaklaşık olarak 854 plaintext-ciphertext çifti ile differential cryptanalysis yapılabilmektedir. Rasgele üretilen 854 çift sonucunda, uygulanan differential cryptanalysis yönteminin son round subkey'ini doğru olarak bulduğu gözlemlenmiştir.

BLOCK CIPHER 2

ΔU_1 : 24576 ➔ 0110 0000 0000 0000
ΔV_1 : 16384 ➔ 0100 0000 0000 0000 $\epsilon_1 = 6 / 16 = 0.375$
ΔU_2 : 2048 ➔ 0000 1000 0000 0000
ΔV_2 : 2048 ➔ 0000 1000 0000 0000 $\epsilon_1 = 4 / 16 = 0.25$
ΔU_3 : 16384 ➔ 0100 0000 0000 0000
ΔV_3 : 24576 ➔ 0110 0000 0000 0000 $\epsilon_1 = 6 / 16 = 0.375$
ΔU_4 : 2176 ➔ 0000 1000 1000 0000

$\pi\epsilon = 0.375 \times 0.25 \times 0.375 = 0.03515625$
Plaintext-ciphertext çift sayısı = 20 / 0.03515625 ≈ 569

```
DIFFERENTIAL ANALYSIS OF SPN BLOCK CİPHER 2

Differential Table of SPN Block Cipher 2
    0   1   2   3   4   5   6   7   8   9   A   B   C   D   E   F
  ____________________________________________________________________
0 |  16  0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
1 |  0   2   2   2   0   0   2   0   0   0   2   0   0   2   2   2
2 |  0   2   2   2   0   0   0   2   0   2   0   0   4   0   2   0
3 |  0   2   2   0   2   0   2   0   4   0   0   0   0   0   2   2
4 |  0   0   0   2   0   2   6   2   0   0   2   0   0   2   0   0
5 |  0   0   0   0   2   4   0   2   2   0   0   2   4   0   0   0
6 |  0   2   0   2   6   0   2   0   0   0   4   0   0   0   0   0
7 |  0   0   2   0   2   2   0   2   2   2   0   2   0   0   2   0
8 |  0   0   0   4   0   2   0   2   4   0   0   0   0   2   0   2
9 |  0   0   2   0   0   0   0   2   0   2   2   2   0   2   4   0
A |  0   2   0   0   2   0   4   0   0   2   0   0   2   0   0   4
B |  0   0   0   0   0   2   0   2   0   2   0   2   2   2   2   2
C |  0   0   4   0   0   4   0   0   0   0   2   2   0   0   2   2
D |  0   2   0   0   2   0   0   0   2   2   0   2   0   4   0   2
E |  0   2   2   2   0   0   0   2   0   4   0   2   2   0   0   0
F |  0   2   0   2   0   0   0   0   2   0   4   2   2   2   0   0

Found Differential Expression:
24576 X 2176 ==> 0,03515625

Found Partial Key:
0000 1011 1101 0000

DIFFERENTIAL ANALYSIS OF SPN BLOCK CİPHER 2 HAS COMPLETED
```

BLOCK CIPHER 3

ΔU_1 : 4 ➔ 0000 0000 0000 0100
ΔV_1 : 6 ➔ 0000 0000 0000 0110 $\epsilon_1 = 6 / 16 = 0.375$
ΔU_2 : 6 ➔ 0000 0000 0000 0110
ΔV_2 : 4 ➔ 0000 0000 0000 0100 $\epsilon_1 = 6 / 16 = 0.375$
ΔU_3 : 4 ➔ 0000 0000 0000 0100
ΔV_3 : 6 ➔ 0000 0000 0000 0110 $\epsilon_1 = 6 / 16 = 0.375$
ΔU_4 : 6 ➔ 0000 0000 0000 0110

$\pi\epsilon = 0.375 \times 0.375 \times 0.375 = 0.052734375$
Plaintext-ciphertext çift sayısı = 20 / 0.052734375 ≈ 380

```
DIFFERENTIAL ANALYSIS OF SPN BLOCK CİPHER 3

Differential Table of SPN Block Cipher 3
    0   1   2   3   4   5   6   7   8   9   A   B   C   D   E   F
  ____________________________________________________________________
0 |  16  0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
1 |  0   2   2   2   0   0   2   0   0   0   2   0   0   2   2   2
2 |  0   2   2   2   0   0   0   2   0   2   0   0   4   0   2   0
3 |  0   2   2   0   2   0   2   0   4   0   0   0   0   0   2   2
4 |  0   0   0   2   0   2   6   2   0   0   2   0   0   2   0   0
5 |  0   0   0   0   2   4   0   2   2   0   0   2   4   0   0   0
6 |  0   2   0   2   6   0   2   0   0   0   4   0   0   0   0   0
7 |  0   0   2   0   2   2   0   2   2   2   0   2   0   0   2   0
8 |  0   0   0   4   0   2   0   2   4   0   0   0   0   2   0   2
9 |  0   0   2   0   0   0   0   2   0   2   2   2   0   2   4   0
A |  0   2   0   0   2   0   4   0   0   2   0   0   2   0   0   4
B |  0   0   0   0   0   2   0   2   0   2   0   2   2   2   2   2
C |  0   0   4   0   0   4   0   0   0   0   2   2   0   0   2   2
D |  0   2   0   0   2   0   0   0   2   2   0   2   0   4   0   2
E |  0   2   2   2   0   0   0   2   0   4   0   2   2   0   0   0
F |  0   2   0   2   0   0   0   0   2   0   4   2   2   2   0   0

Found Differential Expression:
4 X 6 ==> 0,052734375

Found Partial Key:
0000 0000 0000 0100

DIFFERENTIAL ANALYSIS OF SPN BLOCK CİPHER 3 HAS COMPLETED
```

Block cipher 3 için yapılan differential cryptanalysis sonucunda bulunan partial subkey'in doğru olmadığı gözlemlenmiştir. Bu block cipher'ın differential cryptanalysis'inde kullanılan plaintext-ciphertext sayısı arttılmış ve farklı diferansiyel karakteristikleri denenmiştir. Fakat differential cryptanalysis sonucunda bulunan partial key değişmemiştir.

SONUÇ

Block cipher 1 ile block cipher 2 arasındaki fark, iki block cipher'ın farklı substitution kutusu yapılarına sahip olmasıdır. İki block cipher'ın permütasyon katmanı aynıdır. Differential cryptanalysis sonuçlarında da görüldüğü gibi, substitution kutularının tasarımının sonuca doğrudan etkisi vardır. İki block cipher için bulunan diferansiyel karakteristikler karşılaştırıldığına block cipher 1'in diferansiyel karakteristiğinin ihtimalinin block cipher 2'nin karakteristiğinin ihtimalinden daha düşük olduğu gözlemlenmiştir. Bu durum, block cipher 1'in substitution kutularının block cipher 2'ye göre daha iyi tasarlandığını göstermektedir. Block cipher 2'nin karakteristiğinin ihtimali daha yüksek olduğu için, kullanılması gereken plaintext-ciphertext sayısı daha azdır. Bundan ötürü, block cipher 2'nin kırılması block cipher 1'in kırılmasına göre daha kolaydır.

Block cipher 2 ile block cipher 3 arasındaki fark, iki block cipher'ın farklı permütasyon katmanlarına sahip olmasıdır. İki block cipher'da da kullanılan substitution kutuları aynıdır. Block cipher 3'ün permütasyon katmanı incelendiğinde, bir önceki substitution kutularının çıkışlarının bir sonraki substitution kutularının girişlerin doğrudan bağlandığı görülmektedir. Bu durum aslında block cipher 3'te herhangi bir permütasyon uygulanmadığını göstermektedir. İki block cipher'ın sonuçlarına bakıldığına, permütasyon katmanının iyi tasarlanmasının büyük önem arz ettiği görülmektedir. Block cipher 3'te permütasyon katmanı bulunmadığı için, diferansiyel karakteristiğinin ihtimalinin block cipher 2'ye göre daha yüksek olduğu görülmektedir. Bu nedenle block cipher 3'e uygulanacak differential cryptanalysis'te daha az plaintext-ciphertext çiftine gerek duyulacağı gözlemlenmiştir.

Verilen 3 block cipher incelendiğinde, içlerinde en iyisinin block cipher 1 ve en kötüsünün block cipher 3 olduğu söylenebilir.

Ödevde kullanılan tüm kodlar github'a yüklenmiştir: [qua11q7/Cryptography-Homework2]