



# Bilgi Güvenliği ve Kriptoloji

Öğrenci : *Sahil Rzayev 399973*

# RSA

## 1. Anahtar Üretimi

- ✓  $p$  ve  $q$  asal sayıları kullanıcı tarafından ekrana giriliyor.
- ✓ Buna göre de program tüm uygun  $e$  değerlerinin bir listesini kullanıcıya sunuyor ve kullanıcı seçtiği  $e$  değerine göre  $d$  değeri de otomatik program tarafından hesaplanıyor.
- ✓ Tüm bunlar sonucunda ekrana **Genel** ve **Özel anahtar** değerleri basılıyor.

```
Bir asal p sayısı giriniz : 37
Bir asal q sayısı giriniz : 53

----- Seçilebilecek sayılar(e) -----
5 7 11 17 19 23 25 29 31 35 37 41 43 47 49 53 55 59 61 67 71 73 77 79 83 85 89 95 97 101 103 107 109 113 115 119 121 125
127 131 133 137 139 145 149 151 155 157 161 163 167 173 175 179 181 185 187 191 193 197 199 203 205 209 211 215 217 223
227 229 233 235 239 241 245 251 253 257 259 263 265 269 271 275 277 281 283 287 289 293 295 301 305 307 311 313 317 319
323 329 331 335 337 341 343 347 349 353 355 359 361 365 367 371 373 379 383 385 389 391 395 397 401 407 409 413 415 419
421 425 427 431 433 437 439 443 445 449 451 457 461 463 467 469 473 475 479 485 487 491 493 497 499 503 505 509 511 515
517 521 523 527 529 535 539 541 545 547 551 553 557 563 565 569 571 575 577 581 583 587 589 593 595 599 601 605 607 613
617 619 623 625 629 631 635 641 643 647 649 653 655 659 661 665 667 671 673 677 679 683 685 691 695 697 701 703 707 709
713 719 721 725 727 731 733 737 739 743 745 749 751 755 757 761 763 769 773 775 779 781 785 787 791 797 799 803 805 809
811 815 817 821 823 827 829 833 835 839 841 847 851 853 857 859 863 865 869 875 877 881 883 887 889 893 895 899 901 905
907 911 913 917 919 925 929 931 935 937 941 943 947 953 955 959 961 965 967 971 973 977 979 983 985 989 991 995 997 100
3 1007 1009 1013 1015 1019 1021 1025 1031 1033 1037 1039 1043 1045 1049 1051 1055 1057 1061 1063 1067 1069 1073 1075 108
1 1085 1087 1091 1093 1097 1099 1103 1109 1111 1115 1117 1121 1123 1127 1129 1133 1135 1139 1141 1145 1147 1151 1153 115
9 1163 1165 1169 1171 1175 1177 1181 1187 1189 1193 1195 1199 1201 1205 1207 1211 1213 1217 1219 1223 1225 1229 1231 123
7 1241 1243 1247 1249 1253 1255 1259 1265 1267 1271 1273 1277 1279 1283 1285 1289 1291 1295 1297 1301 1303 1307 1309 131
5 1319 1321 1325 1327 1331 1333 1337 1343 1345 1349 1351 1355 1357 1361 1363 1367 1369 1373 1375 1379 1381 1385 1387 139
3 1397 1399 1403 1405 1409 1411 1415 1421 1423 1427 1429 1433 1435 1439 1441 1445 1447 1451 1453 1457 1459 1463 1465 147
1 1475 1477 1481 1483 1487 1489 1493 1499 1501 1505 1507 1511 1513 1517 1519 1523 1525 1529 1531 1535 1537 1541 1543 154
9 1553 1555 1559 1561 1565 1567 1571 1577 1579 1583 1585 1589 1591 1595 1597 1601 1603 1607 1609 1613 1615 1619 1621 162
7 1631 1633 1637 1639 1643 1645 1649 1655 1657 1661 1663 1667 1669 1673 1675 1679 1681 1685 1687 1691 1693 1697 1699 170
5 1709 1711 1715 1717 1721 1723 1727 1733 1735 1739 1741 1745 1747 1751 1753 1757 1759 1763 1765 1769 1771 1775 1777 178
3 1787 1789 1793 1795 1799 1801 1805 1811 1813 1817 1819 1823 1825 1829 1831 1835 1837 1841 1843 1847 1849 1853 1855 186
1 1865 1867 1871
e sayısı seçiniz : 1793

Genel anahtar(n:1961,e:1793)

Özel anahtar(d:545)

Metin giriniz : kriptoloji dersi odev sunumu
```

## 2.Şifreleme

- ✓ Genel anahtarla(n,e) şifreleme yapıldı(gönderici genel anahtarla mesajı şifreliyor).
- ✓ ASCII değerlerinin basamak sayıları **L\_clear** ve **L\_cipher**'e (şifreli metnindeki ascii değerlerinin basamak sayısı) göre ayarlandı.

```
----- Şifreleme -----

uc basamaklı  ascii değerler
107      114      105      112      116      111      108      111      106      105      032      100      101      114      115
105      032      111      100      101      118      032      115      117      110      117      109      117      5

L_clear'a göre ayarlanmış (string türünde) ascii değerler
107      114      105      112      116      111      108      111      106      105      032      100      101      114      115
105      032      111      100      101      118      032      115      117      110      117      109      117

L_clear'a göre ayarlanmış (int türünde) ascii değerler
107      114      105      112      116      111      108      111      106      105      32      100      101      114      115
105      32      111      100      101      118      32      115      117      110      117      109      117

mod alınmış değerler - n:1961 d:1793
1644      139      105      963      1182      74      1563      74      742      105      631      1157      85      139      1649
105      631      74      1157      85      234      631      1649      1301      517      1301      1678      1301

Basamak sayısı L_cipher'a göre ayarlı
Şifrelenmiş Metin
1644013901050963118200741563007407420105063111570085013916490105063100741157008502340631164913010517130116781301
```

### 3.Deşifreleme

- ✓ **Özel anahtarla(d)** deşifreleme yapıldı(alıcı özel anahtarla mesajı deşifreliyor).
- ✓ ASCII değerlerinin basamak sayıları **L\_clear** ve **L\_cipher**'e göre ayarlandı

```
----- Deşifreleme -----

Şifrelenmiş metnin deşifrelemeye aktarılması
1644  0139  0105  0963  1182  0074  1563  0074  0742  0105  0631  1157  0085  0139  1649
0105  0631  0074  1157  0085  0234  0631  1649  1301  0517  1301  1678  1301

Şifrelenmiş metnin integer halinde kullanılması
1644  139  105  963  1182  74  1563  74  742  105  631  1157  85  139  1649
105  631  74  1157  85  234  631  1649  1301  517  1301  1678  1301

mod alınmış değerler - n:1961 e:545
107  114  105  112  116  111  108  111  106  105  32  100  101  114  115
105  32  111  100  101  118  32  115  117  110  117  109  117

L_clear basamaklı tek tek desifrelenmiş değerler
107  114  105  112  116  111  108  111  106  105  032  100  101  114  115
105  032  111  100  101  118  032  115  117  110  117  109  117

desifrelenmiş uclu ascii değerler
107  114  105  112  116  111  108  111  106  105  032  100  101  114  115
105  032  111  100  101  118  032  115  117  110  117  109  117

Çözülmüş Metin
107114105112116111108111106105032100101114115105032111100101118032115117110117109117
```

## 4.Mesaj Doğrulaması

- Göndericinin gönderdiği mesajla alıcının elde ettiği mesaj aynıdırsa yeşil rengli “Mesaj doğrulandı” yazısı ekrana basılacak.

Gönderilmiş mesaj  
kriptoloji dersi odev sunumu

Alınmış mesaj  
kriptoloji dersi odev sunumu

Mesaj doğrulandı

# DES

## 1.Şifreleme

- Kullanıcı metni giriyor. Girilen metin ilk olarak **başlangıç permütasyon(IP)** uygulanıyor. Sonra 32 bitlik iki alt bloğa bölünüyor.
- Daha sonra 16 döngü uygulanıyor. Her döngüde anahtar bitlerinden 56'dan 48'i seçiliyor. Bloğun sağ yarısı **genişletme permütasyonu(EP)** ile 48 bite(32 bitden 48 bite genişletme) genişletip, **XOR** işlemi uygulanarak anahtarla birleştiriliyoruz.
- Elde edilen sonuç **S-box**'lara gönderilerek 32 yeni bit üretiliyor ve yeniden tekrar **permütasyon(D-box)** uygulanıyor. Elde edilen sonuç bloğun sol yarısı ile birleştirilerek **XOR** yapılır ve **sağ blok** olarak atanır.
- **Sol blok** sağ bloğun döngüye başlangıcındaki halidir.
- 16 döngüden sonra bir sonraki 64 bitlik bloğa geçilir. En sonda başlangıçta uygulanan permütasyonun tersi(**IP1**) uygulanır.

Text: 123412AB123412AB

Encryption:

İlk permütasyondan sonra : 0077228888AA88DD

Böldükten sonra : L0=00772288 R0=88AA88DD

Döngü 1 88AA88DD B58385D8 194CD072DE8C  
Döngü 2 B58385D8 72B42488 4568581ABCCE  
Döngü 3 72B42488 4AB4A0B2 06EDA4ACF5B5  
Döngü 4 4AB4A0B2 DB5D80D7 DA2D032B6EE3  
Döngü 5 DB5D80D7 7E5D4F8C 69A629FEC913  
Döngü 6 7E5D4F8C 3980257D C1948E87475E  
Döngü 7 3980257D 593B0610 708AD2DDB3C0  
Döngü 8 593B0610 6E9E2886 34F822F0C66D  
Döngü 9 6E9E2886 E73258AD 84BB4473DCCC  
Döngü 10 E73258AD 3E9BD9AC 02765708B5BF  
Döngü 11 3E9BD9AC B4094DC9 6D5560AF7CA5  
Döngü 12 B4094DC9 8DC4E402 C2C1E96A4BF3  
Döngü 13 8DC4E402 F7899B14 99C31397C91F  
Döngü 14 F7899B14 4A2AAA50 251B8BC717D0  
Döngü 15 4A2AAA50 649A5432 3330C5D9A36D  
Döngü 16 649A5432 03F92C8E 181C5D75C66D

Cipher Text: 50638D353A969831

## 2.Deşifreleme

- Şifrelemeden alınan şifrelenmiş metin çözülmesi için deşifrelemeye dahil ediliyor. Burada da şifrelemdeki adımların aynısı uygulanıyor. Tek fark 16 döğüden uygulanan anahtar sırası tersden uygulanıyor.

Decryption

İlk permütasyondan sonra : 03F92C8E649A5432

Böldükten sonra : L0=03F92C8E R0=649A5432

Döngü 1 649A5432 4A2AAA50 181C5D75C66D  
Döngü 2 4A2AAA50 F7899B14 3330C5D9A36D  
Döngü 3 F7899B14 8DC4E402 251B8BC717D0  
Döngü 4 8DC4E402 B4094DC9 99C31397C91F  
Döngü 5 B4094DC9 3E9BD9AC C2C1E96A4BF3  
Döngü 6 3E9BD9AC E73258AD 6D5560AF7CA5  
Döngü 7 E73258AD 6E9E2886 02765708B5BF  
Döngü 8 6E9E2886 593B0610 84BB4473DCCC  
Döngü 9 593B0610 3980257D 34F822F0C66D  
Döngü 10 3980257D 7E5D4F8C 708AD2DDB3C0  
Döngü 11 7E5D4F8C DB5D80D7 C1948E87475E  
Döngü 12 DB5D80D7 4AB4A0B2 69A629FEC913  
Döngü 13 4AB4A0B2 72B42488 DA2D032B6EE3  
Döngü 14 72B42488 B58385D8 06EDA4ACF5B5  
Döngü 15 B58385D8 88AA88DD 4568581ABCCE  
Döngü 16 88AA88DD 00772288 194CD072DE8C

Plain Text: 123412AB123412AB

BUILD SUCCESSFUL (total time: 0 seconds)



# DSA (Sayısal İmza)

DSA Asimetrik şifreleme için RSA algoritması kullanıldı. **DSA**'nın **RSA**'dan farkı:

- Kullanıcı **RSA**'da girdiği metnin ASCII değerlerine göre **RSA** hesaplanırken, **DSA**'da kullanıcı'nın girdiği metnin hash'lenmiş değerlerinin ASCII değerlerine göre **DSA** hesaplanıyor.
- Diğer bir farkı **RSA**'da **genel anahtarla şifreleme** yapıp, **özel anahtarla deşifreleme** yapıyoruz, ama **DSA**'da **özel anahtarla şifreleme** yapıp, **genel anahtarla deşifreliyoruz**.

# 1. Anahtar Üretimi

- ✓ **p** ve **q** asal sayıları kullanıcı tarafından ekrana giriliyor.
- ✓ **d** ve **e** değerleri otomatik program tarafından hesaplanıyor.
- ✓ Tüm bunlar sonucunda ekrana **Genel(n,e)** ve **Özel(d)** **anahtar** değerleri basılıyor.

```
Bir asal p sayısı giriniz : 37  
Bir asal q sayısı giriniz : 53
```

```
Genel anahtar(n:1961,d:85)
```

```
Özel anahtar(e:925)
```

```
Metin giriniz : kriptoloji dersi odev sunumu
```

```
Hash
```

```
8c79da4827fa61ef73681f1d348f426eddf207fd5db7418044aaa0ab1fae4c61
```

## 2.Şifreleme

- ✓ Özel anahtarla(d) şifreleme yapıldı(gönderici özel anahtarla mesajı şifreliyor).
- ✓ ASCII değerlerinin basamak sayıları **L\_clear** ve **L\_cipher**'e (şifreli metnindeki ascii değerlerinin basamak sayısı) göre ayarlandı.

```
----- Şifreleme -----

uc basamaklı  ascii değerler

056      099      055      057      100      097      052      056      050      055      102      097      054      049
101      102      055      051      054      056      049      102      049      100      051      052      056      102
052      050      054      101      100      100      102      050      048      055      102      100      053      100
098      055      052      049      056      048      052      052      097      097      097      048      097      098
049      102      097      101      052      099      054      049

L_clear'a göre ayarlanmış (string türünde) ascii değerler

056      099      055      057      100      097      052      056      050      055      102      097      054      049
101      102      055      051      054      056      049      102      049      100      051      052      056      102
052      050      054      101      100      100      102      050      048      055      102      100      053      100
098      055      052      049      056      048      052      052      097      097      097      048      097      098
049      102      097      101      052      099      054      049

L_clear'a göre ayarlanmış (int türünde) ascii değerler

56       99       55       57       100      97       52       56       50       55       102      97       54       49
101      102      55       51       54       56       49       102      49       100      51       52       56       102
52       50       54       101      100      100      102      50       48       55       102      100      53       100
98       55       52       49       56       48       52       52       97       97       97       48       97       98
49       102      97       101      52       99       54       49

mod alınmış değerler - n:1961 d:85

1152     872     402     113     63      652     1907     1152     1869     402     99      652     849     682
1063     99      402     976     849     1152     682     99      682     63      976     1907     1152     99
1907     1869     849     1063     63      63      99      1869     1010     402     99      63      1378     63
684      402     1907     682     1152     1010     1907     1907     652     652     652     1010     652     684
682      99      652     1063     1907     872     849     682

Basamak sayısı L_cipher'a göre ayarlı

Şifrelenmiş Metin

1152087204020113006306521907115218690402009906520849068210630099040209760849115206820099068200630976190711520099
1907186908491063006300630099186910100402009900631378006306840402190706821152101019071907065206520652101006520684
06820099065210631907087208490682
```

### 3. Deşifreleme

- ✓ Genel anahtarla( $n, e$ ) deşifreleme yapıldı(alıcı genel anahtarla mesajı deşifreliyor).
- ✓ ASCII değerlerinin basamak sayıları  $L\_clear$  ve  $L\_cipher$ 'e göre ayarlandı.

```
----- Deşifreleme -----  
  
Şifrelenmiş metnin deşifrelemeye aktarılması  
1152 0872 0402 0113 0063 0652 1907 1152 1869 0402 0099 0652 0849 0682  
1063 0099 0402 0976 0849 1152 0682 0099 0682 0063 0976 1907 1152 0099  
1907 1869 0849 1063 0063 0063 0099 1869 1010 0402 0099 0063 1378 0063  
0684 0402 1907 0682 1152 1010 1907 1907 0652 0652 0652 1010 0652 0684  
0682 0099 0652 1063 1907 0872 0849 0682  
  
Şifrelenmiş metnin integer halinde kullanılması  
1152 872 402 113 63 652 1907 1152 1869 402 99 652 849 682  
1063 99 402 976 849 1152 682 99 682 63 976 1907 1152 99  
1907 1869 849 1063 63 63 99 1869 1010 402 99 63 1378 63  
684 402 1907 682 1152 1010 1907 1907 652 652 652 1010 652 684  
682 99 652 1063 1907 872 849 682  
  
mod alınmış değerler - n:1961 e:925  
  
tek tek desifrelenmiş(mod alınmış) değerler  
56 99 55 57 100 97 52 56 50 55 102 97 54 49  
101 102 55 51 54 56 49 102 49 100 51 52 56 102  
52 50 54 101 100 100 102 50 48 55 102 100 53 100  
98 55 52 49 56 48 52 52 97 97 97 48 97 98  
49 102 97 101 52 99 54 49
```

L\_clear basamaklı tek tek desifrelenmiş değerler

056	099	055	057	100	097	052	056	050	055	102	097	054	049
101	102	055	051	054	056	049	102	049	100	051	052	056	102
052	050	054	101	100	100	102	050	048	055	102	100	053	100
098	055	052	049	056	048	052	052	097	097	097	048	097	098
049	102	097	101	052	099	054	049						

desifrelenmiş uclu ascii değerler

056	099	055	057	100	097	052	056	050	055	102	097	054	049
101	102	055	051	054	056	049	102	049	100	051	052	056	102
052	050	054	101	100	100	102	050	048	055	102	100	053	100
098	055	052	049	056	048	052	052	097	097	097	048	097	098
049	102	097	101	052	099	054	049						

Çözülmüş Metin

0560990550571000970520560500551020970540491011020550510540560491020491000510520561020520500541011001001020500480  
55102100053100098055052049056048052052097097097048097098049102097101052099054049