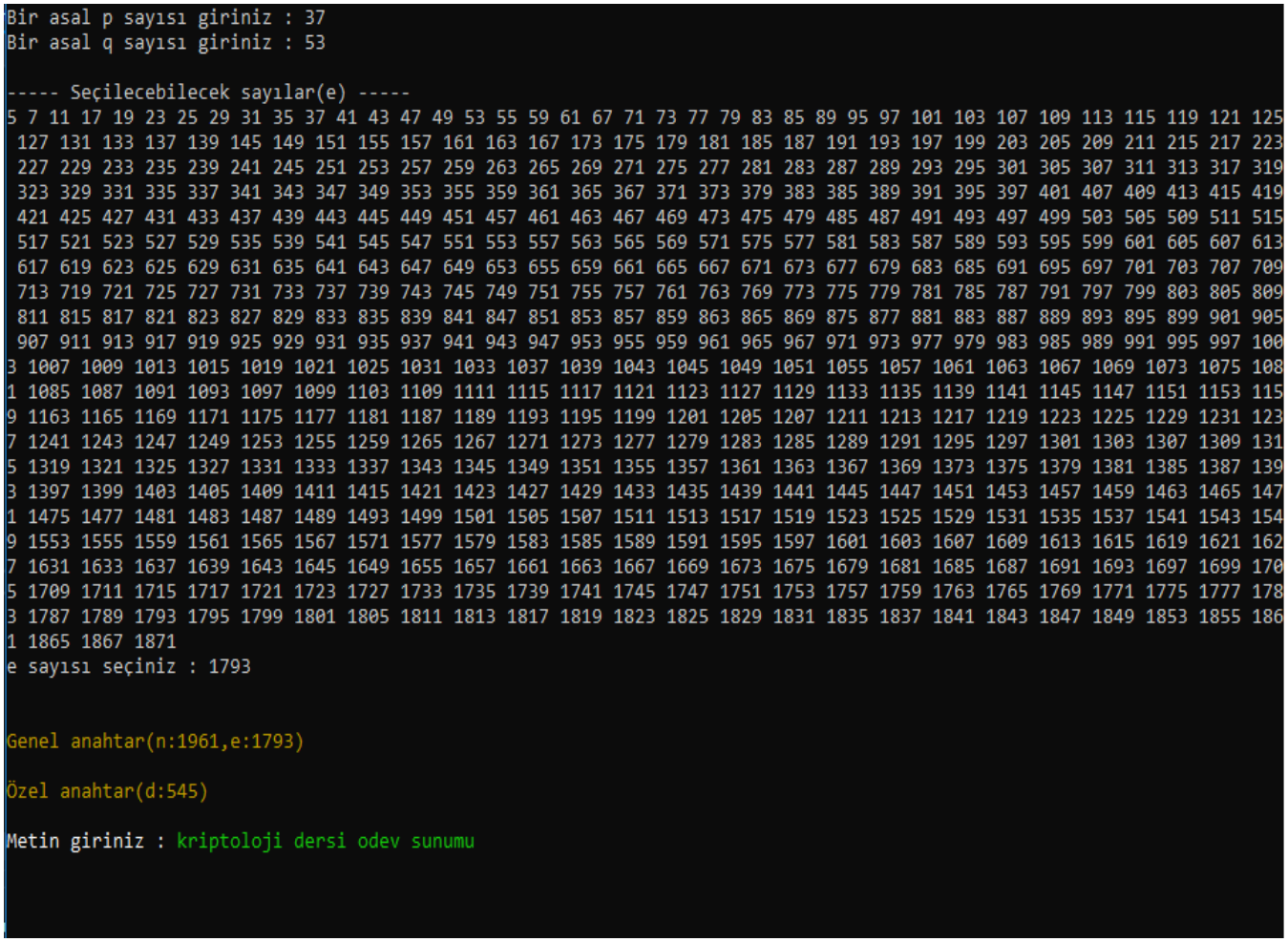
Bilgi Güvenliği ve Kriptoloji

Öğrenci : ***Sahil Rzayev 399973***

RSA

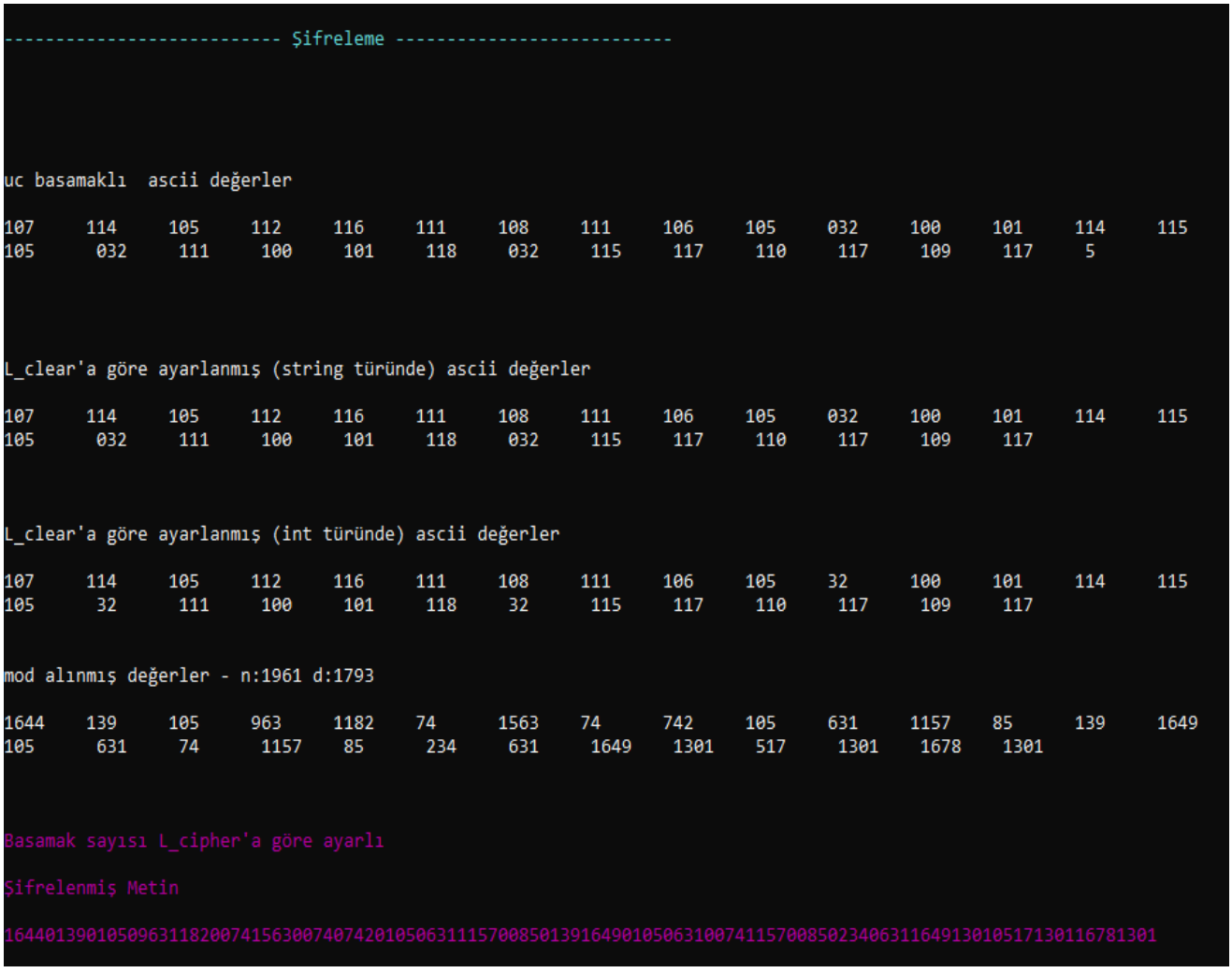
1.Anahtar Üretimi

- ✓ **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.



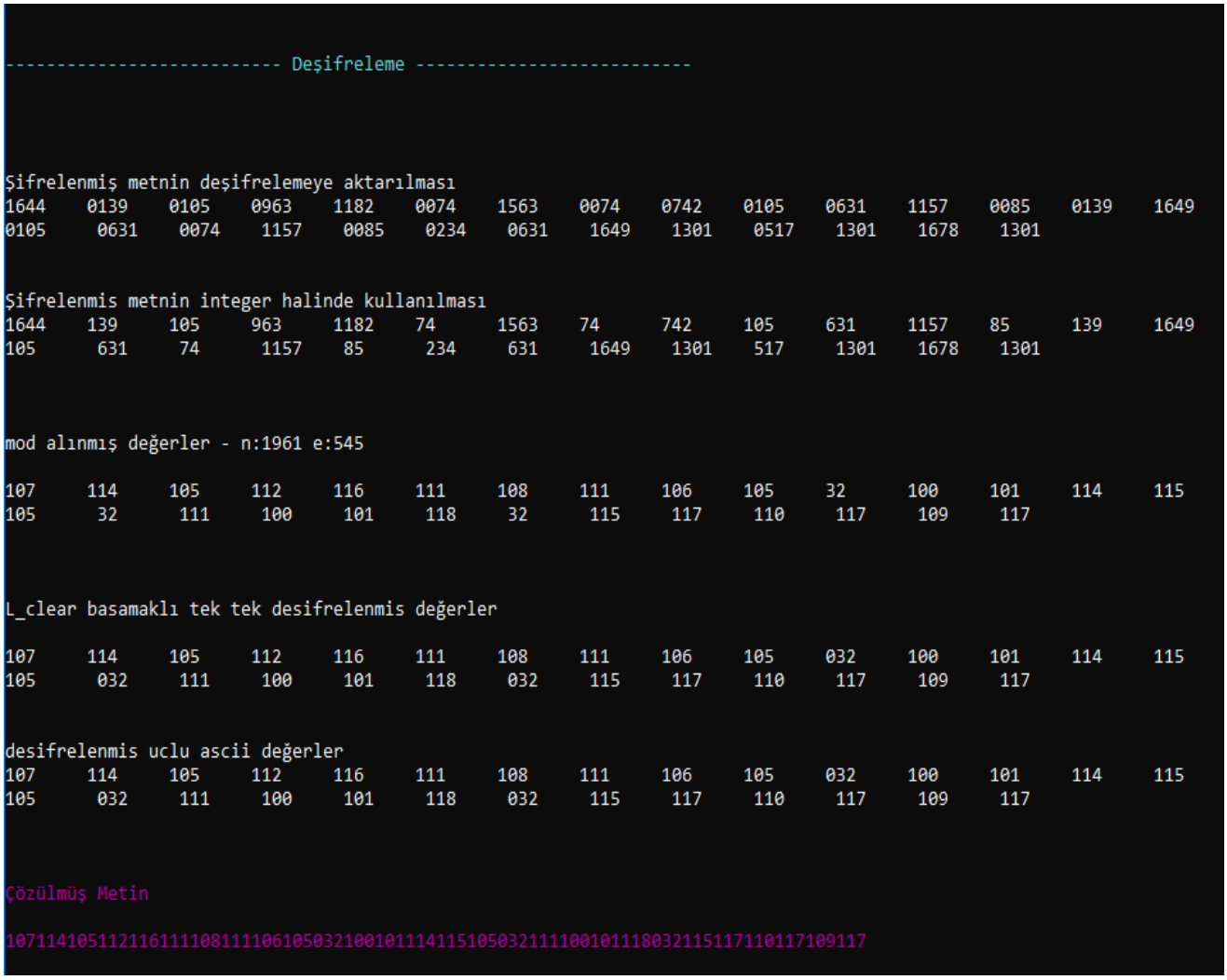
2.Şifreleme

- ✓ **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.



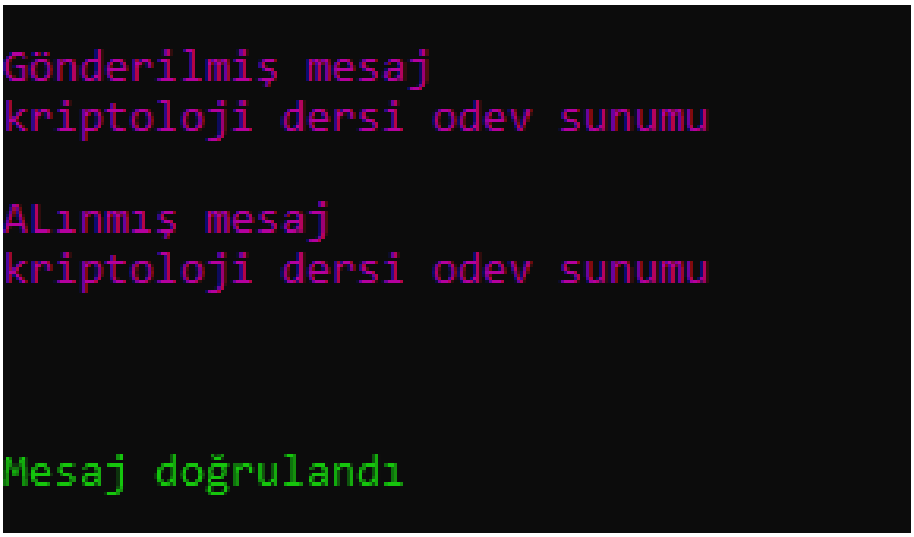
3.Deşifreleme

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



4.Mesaj Doğrulaması

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



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 blo**k 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 dögüden 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)
```

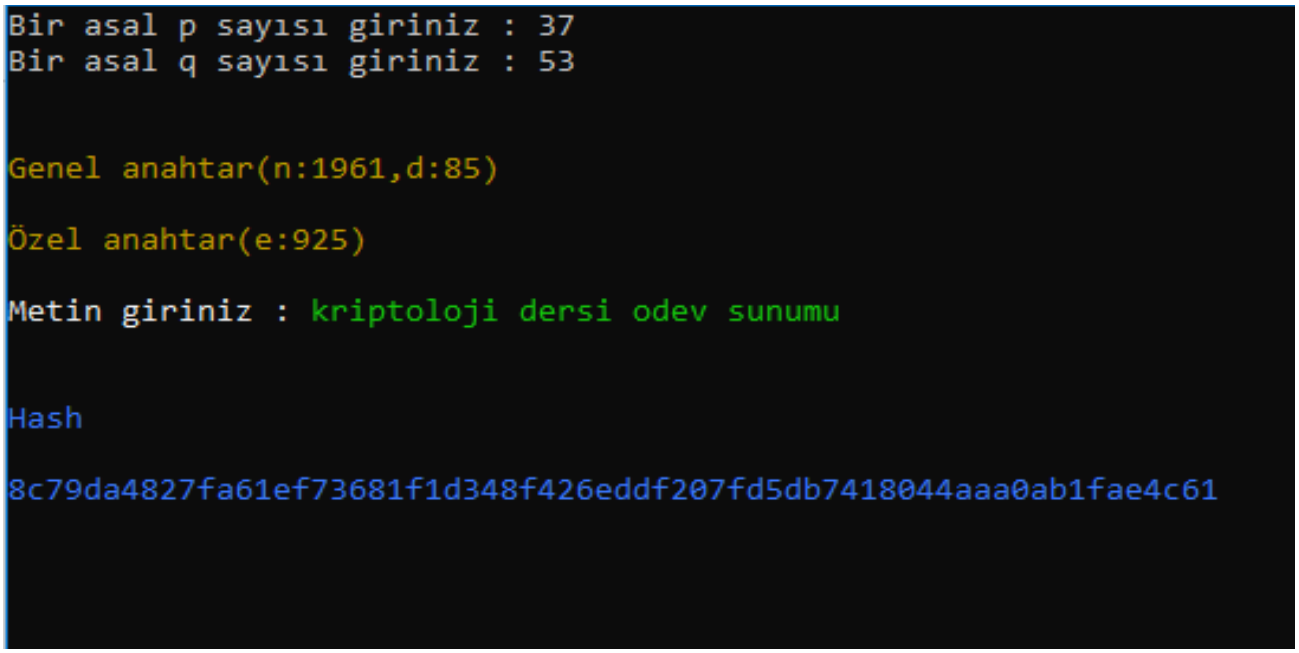
DSA (Sayısal İmza)

DSA Asimmetrik 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.



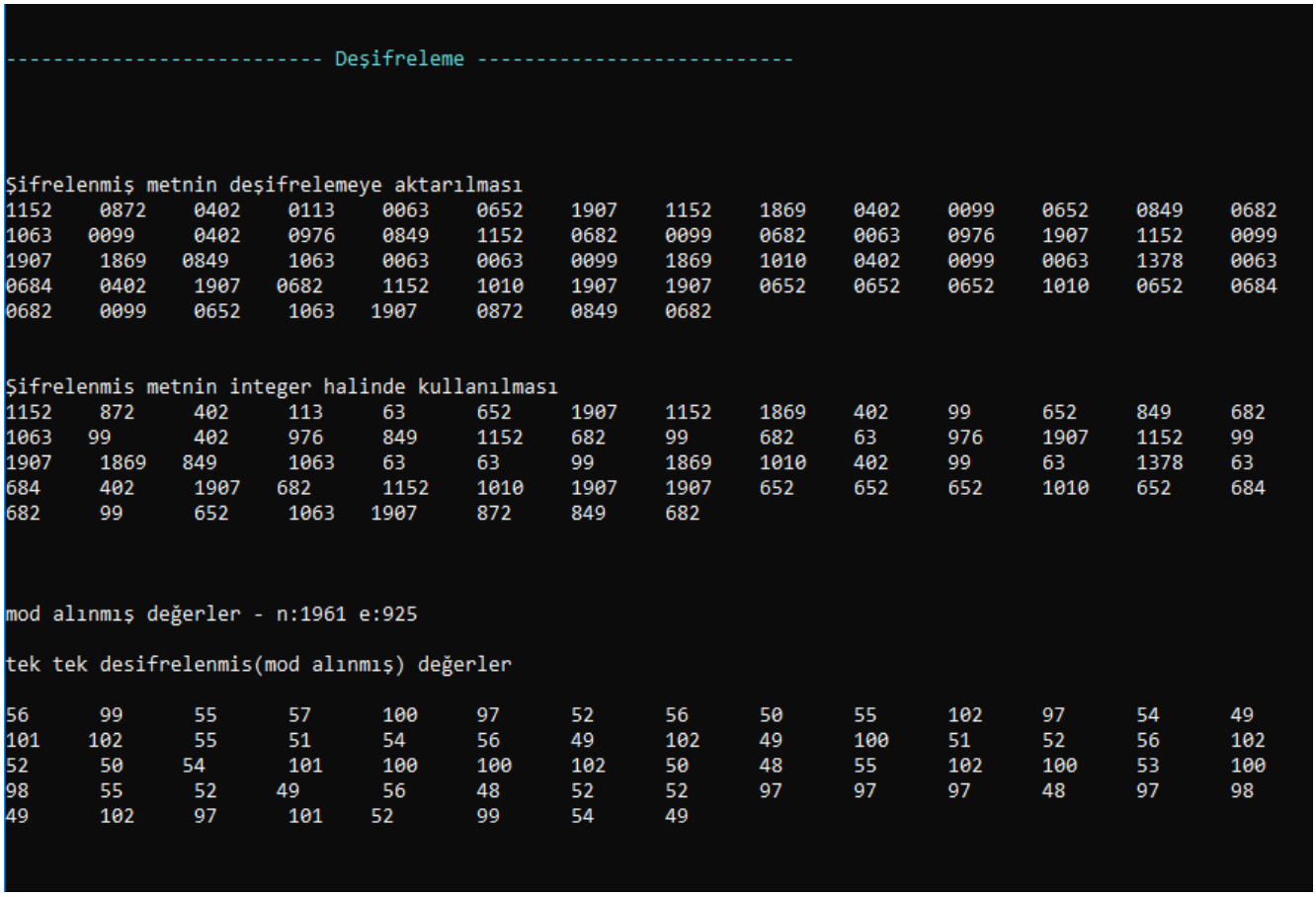
2.Şifreleme

- ✓ **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

115208720402011300630652190711521869040200990652084906821063009904020976084911520682009906820063097619071152009919071869084910630063006300991869101004020099006313780063068404021907068211521010190719070652065206521010065206840682009906521063190708720849068 2
```

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.



```
L_clear basamaklı tek tek desifrelenmis 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


desifrelenmis 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

056099055057100097052056050055102097054049101102055051054056049102049100051052056102052050054101100100102050048055102100053100098055052049056048052052097097097048097098049102097101052099054049
```