

RSA Public-Key Encryption and Digital Signature Applications:

- README file about code is in ‘rsa’ path with this document’s zip.

Task 1:

```
[06/25/22]seed@VM:~/shared$ ./rsa_task1.out
The plaintext --> 4163617969702067697A6C6920626972206D6573616A21
Encrypted --> 2A3E2EEA928A52FF0A299493750EFDEE95394998D85E4484F68399222EC
F515F1FC86813A19A2EBEE1C802C45959254B3D2D9D4F502BD249B9D094E0A2B954B6
Decrypted (to provide) --> 4163617969702067697A6C6920626972206D6573616A21
Hex mean of decrypted --> Acayip gizli bir mesaj!
```

Task 2:

```
### TASK 2 ###
Derived public key (n) from p and q is --> BB300643E39AA365612115898C2737D9
69635148A40AAAD9F2A92E60A7BB1BB7DA9A09F339FE02761FF451FF0FAFAFEA1C792D3C0114
B2D4234FCFEABF1249C1
Derived private key (d) from p, q and e is --> 89719CD812724451B73CECAC7F7D
7873A9FF63FABB809DACC491D6DCDFABF2900C62135A3F0795B111DF706E0453D70E23CA4713
843836F89BFDB5941302C765
The plaintext --> 427520646120696B696E63692067697A6C69206D6573616A
Encrypted --> 85F35845F92B7FD091FF77E9AB80DF682E54A9868804AC28284652D766912
FAF868BC755DD800F47CFC683EBF4BCD092C51366A7124F8E852B0DEF1ACE7169D7
Decrypted (to provide) --> 427520646120696B696E63692067697A6C69206D6573616A
Hex mean of decrypted --> Bu da ikinci gizli mesaj
```

Task 3:

```
### TASK 3 ###
-- p, q, e (therefore derived d and n) values are same with task 2.--
The ciphertext --> 7AA0FF25F5D5C94FBEA7109F8AA34A43ADA883EF30CE12A4595BBD92
D36D91FBE43A841400345177D6572F6587882FAB78549D6155500F9D319F892F8E74F07F
Decrypted --> 42756C64756D2067697A6C69206D6573616A6921
Hex mean of decrypted --> Buldum gizli mesaji!
```

Task 4:

```
### TASK 4 ###
-- p, q, e (therefore derived d and n) values are same with task 2.--
Signature --> B5A03FF24C062885FBA9B86511CAB4EEE33A636B2C128ECFA50B32A8110BAE364535CB
E1FC49DD80E2E3947ADF2363089BED928DDC56C441A941508F87B4E81
Signature for changed text (1 to 2) --> 90F8AF63521E0E9C3039E3623C3C9371963DE18D4B85
7FB6D3978DC64ED279C23B7DC301F059EBAEF7356E0B46735BADE09D285A4C768831BDA35238B6F8FEE8
-- Although we changed a single character in the main text, we noticed a huge change in the signatures of the texts.
Considering that we also obtain the signatures of the texts by encryption, we have seen that a small change in the plaintexts can completely change the ciphertext.--
Decrypted (to provide): 53616E612031206D696C796F6E206C69726120626F7263756D207661722E
Hex mean of decrypted: Sana 1 milyon lira borcum var.
Decrypted of changed text (to provide): 53616E612032206D696C796F6E206C69726120626F72
63756D207661722E
Hex mean of decrypted: Sana 2 milyon lira borcum var.
```

Task 5:

```
[06/25/22]seed@VM:~/shared$ ./rsa_task5.out
Message is: 4C61756E63682061206D697373696C652E
Hex mean of message: Launch a missile.

-- The verification algorithm is to compute S^e mod n and then compare the result with the message M --
Verifying with S1: 4C61756E63682061206D697373696C652E
Hex mean of decrypted S1: Launch a missile.
Verifying with S2: 1E1EBB56ECD7B9E1499DCFEA1088D146A174BB7CA1D754874B814BA175EDCEA
Hex mean of decrypted: 0V00{00000jK00uHt00^00

S1 verified that its the signature of Alice because its decryption gives the message us. Decryption of S2 is meanless.
```

Crypto and Symmetric Key Encryption Applications:

- Files of each task are in ‘crypto’ path with this document’s zip.

Task 1:

- I convert the ciphertext to upper and I analysed the text. I change single letter ‘D’ with ‘a’ and ‘DSS?’ with ‘all?’ first. And changed ‘EY’ to ‘of’, ‘DAC’ to ‘and’ and ‘RUF’ to ‘the’. Other letters opened quickly later.

```
[06/25/22]seed@VM:~/.../task-1$ cat cipher_upper.txt
UO CFDM VRKCFAR,
RUOV OV RUF UEFBEMX YEM RUF JEKMVF EY OARMECKJROEA RE JLZFM VFJKRORL.
REZZ FRK CFNDMRWFA R EY JEWNKRFM FAGAFFMOAG OF RUF YOMVR DAC EASL CFNDMRWFA R YMWE D RKMXOVU KAOPFMVRL BORU OAYEMWDROJV FKMENF WFWZFMVUON.
OAYEMWDROJV FKMENF MFNMVFARV RUF DJDCFWOJ DAC MFVFDMJU JEWWKAORL OA OAYEMWDROJV OA FKMENF DAC AFQGUZEKMOAG JEKARMOFV.
OR DOWV RE OWNMEPF, VUDNF DAC MFPOPF HKDSRL OA MFVFDMJU, FCKJDRDEA DAC XAEBSFCGF RMDAVYFM OA OAYEMWDROJV OA FKMENF ZL ZMOAGOAG REGFRUFM KAOF
FMVORL CFNDMRWFA R DAC MFVFDMJU SDZEMDREM OFV DAC JMFDROAG D VRMEAG KAORL ZFRBFFA RUFW.
ZDVF C OA IKMOJU, VBORIFMSDAC, OAYEMWDROJV FKMENF OV D AEA-NMEYOR JEWWKAORL ZDVF C EA WFWZFMVUON.
RUF WDOA WVOVOEA EY RUF JEWWKAORL OV RE NMWERF MFVFDMJU, FCKJDRDEA DAC XAEBSFCGF RMDAVYFM OA OAYEMWDROJV.
OAYEMWDROJV FKMENF MFNMVFARV EPFM 120 KAOPFMVRL CFNDMRWFA R DAC MFVFDMJU OAVRORKRFV DJMEV AFDSL 30 JEKARMOFV OA FKMENF.
OAYEMWDROJV FKMENF WFWZFMVUON YEM EKM CFNDMRWFA R BOSS NSDL D JMKJODS MESF YEM EKM VRKCFARV OA VUDNOAG RUFOM DJDCFWOJ DAC ZKVOAFVV JDMFFMV OARF
MADROADSSL.
COC LEK MFDC DSS?
LFV, GEEC RUFA...[06/25/22]seed@VM:~/.../task-1$
[06/25/22]seed@VM:~/.../task-1$ tr 'D S A E C Y G R L M W U F O K J Z V B X N P H I' 'a l n o d f g t y r m h e i u c b s w k p v q z' < cipher_upper.txt
hi dear student,
this is the homework for the course of introduction to cyber security.
tobb etu department of computer engineering is the first and only department from a turkish university with informatics europe membership.
informatics europe represents the academic and research community in informatics in europe and neighbouring countries.
it aims to improve, shape and revive quality in research, education and knowledge transfer in informatics in europe by bringing together universities departments and research laboratories and creating a strong unity between them.
based in zurich, switzerland, informatics europe is a non-profit community based on membership.
the main mission of the community is to promote research, education and knowledge transfer in informatics.
informatics europe represents over 120 university departments and research institutes across nearly 30 countries in europe.
informatics europe membership of our department will play a crucial role for our students in shaping their academic and business careers internationally.
did you read all?
yes, good then...[06/25/22]seed@VM:~/.../task-1$
```

Task 2:

- Part 1: Encrypting with three different ciphers (encrypted images and images obtained with ‘cat’ command will be sended with this file)

- AES-128-CFB

```
[06/25/22]seed@VM:~/.../secret$ openssl enc -aes-128-cfb -e \
> -in pic_original.bmp -out pic_aes-128-cfb.bmp \
> -K 00112233445566778899aabcccddeeff -iv 00aa11bb22cc33dd44ee55ff66778899
[06/25/22]seed@VM:~/.../secret$ head -c 54 pic_original.bmp > header
[06/25/22]seed@VM:~/.../secret$ tail -c +55 pic_aes-128-cfb.bmp > body
[06/25/22]seed@VM:~/.../secret$ cat header body > new_pic_aes-128-cfb.bmp
```

- AES-128-CBC

```
[06/25/22]seed@VM:~/.../secret$ openssl enc -aes-128-cbc -e \
> -in pic_original.bmp -out pic_aes-128-cbc.bmp \
> -K 00112233445566778899aabcccddeeff -iv 00aa11bb22cc33dd44ee55ff66778899
[06/25/22]seed@VM:~/.../secret$ head -c 54 pic_original.bmp > header
[06/25/22]seed@VM:~/.../secret$ tail -c +55 pic_aes-128-cbc.bmp > body
[06/25/22]seed@VM:~/.../secret$ cat header body > new_pic_aes-128-cbc.bmp
```

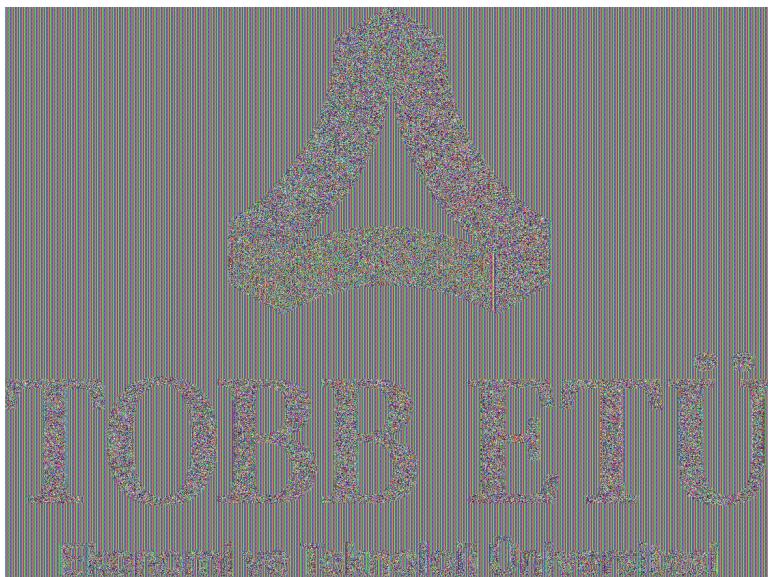
- DES-CBC

```
[06/25/22]seed@VM:~/.../secret$ openssl enc -des-cbc -e \
> -in pic_original.bmp -out pic_des-cbc.bmp \
> -K 0123456789abcdef -iv 0102030405060708
[06/25/22]seed@VM:~/.../secret$ head -c 54 pic_original.bmp > header
[06/25/22]seed@VM:~/.../secret$ tail -c +55 pic_des-cbc.bmp > body
[06/25/22]seed@VM:~/.../secret$ cat header body > new_pic_des-cbc.bmp
```

- **Part 2: Encrypting with ECB and CBC two images, then compare methods**

- o **ECB and CBC on given image (pic_original.bmp)**

```
[06/25/22]seed@VM:~/.../secret$ openssl enc -aes-128-ecb -e \  
> -in pic_original.bmp -out pic_aes-128-ecb.bmp \  
> -K 00112233445566778899aabbccddeeff  
[06/25/22]seed@VM:~/.../secret$ head -c 54 pic_original.bmp > header  
[06/25/22]seed@VM:~/.../secret$ tail -c +55 pic_aes-128-ecb.bmp > body  
[06/25/22]seed@VM:~/.../secret$ cat header body > new_pic_aes-128-ecb.bmp
```



```
[06/25/22]seed@VM:~/.../secret$ openssl enc -bf-cbc -e \  
> -in pic_original.bmp -out pic_bf-cbc.bmp \  
> -K 00112233445566778899aabbccddeeff -iv 0102030405060708  
[06/25/22]seed@VM:~/.../secret$ head -c 54 pic_original.bmp > header  
[06/25/22]seed@VM:~/.../secret$ tail -c +55 pic_bf-cbc.bmp > body  
[06/25/22]seed@VM:~/.../secret$ cat header body > new_pic_bf-cbc.bmp
```



- ECB and CBC on chosen image (besiktas.bmp)

```
[06/25/22]seed@VM:~/.../secret$ openssl enc -aes-128-ecb -e \  
> -in besiktas.bmp -out besiktas_aes-128-ecb.bmp \  
> -K 00112233445566778899aabcccddeeff  
[06/25/22]seed@VM:~/.../secret$ head -c 54 besiktas.bmp > header  
[06/25/22]seed@VM:~/.../secret$ tail -c +55 besiktas_aes-128-ecb.bmp > body  
[06/25/22]seed@VM:~/.../secret$ cat header body > new_besiktas_aes-128-ecb.bmp
```



```
[06/25/22]seed@VM:~/.../secret$ openssl enc -bf-cbc -e \  
> -in besiktas.bmp -out besiktas_bf-cbc.bmp \  
> -K 00112233445566778899aabcccddeeff -iv 0102030405060708  
[06/25/22]seed@VM:~/.../secret$ head -c 54 besiktas.bmp > header  
[06/25/22]seed@VM:~/.../secret$ tail -c +55 besiktas_bf-cbc.bmp > body  
[06/25/22]seed@VM:~/.../secret$ cat header body > new_besiktas_bf-cbc.bmp
```



- Comparing ECB and CBC results

Making out the shapes of encrypted image with using ECB encryption is very easy. When using CBC, I cannot see any relationship between original image and encrypted image. When I repeat the scenario for chosen image (besiktas.bmp), the result were same. The shapes of my encrypted image is open to see when I use ECB.

Task 3:

- Assumption

We know effects of single bit errors on i'th block on modes. In ECB and OFB, it causes a bit error in i'th block. In CBC and CFB, single bit error in a block will cause failure of decryption in subsequent block because they chains all blocks together by XORing the output of the encryption block with the next plaintext block.

In the light of this information, we can say that the most error loss will be in CFB and CBC modes. It is clear that in ECB and OFB modes, there will be minimal loss (In OFB with one bit).

- I created a text file includes “Gençliğe Hitabe”. It is exactly 1399 bytes.

The screenshot shows a terminal window with the following content:

```
seed@VM: ~/task-3$ ls -la myfile.txt
-rwxrwxrwx 1 root root 1399 Jun 25 12:25 myfile.txt
seed@VM:~/task-3$ cat myfile.txt
Ey Türk gençliği!
Birinci vazifen; Türk istiklalini, Türk cumhuriyetini, ilelebet muhafaza ve müdafaa etmektir.
Mevcudiyetinin ve istikbalinin yegâne temeli budur.
Bu temel, senin en kıymetli hazinendir.
İstikbalde dahi seni bu hazineinden mahrum etmek isteyecek dâhilî ve harici bedhahların olacaktır.
Bir gün, istiklal ve cumhuriyeti müdafaa mecburiyetine düşersen, vazifeye atılmak için içinde bulunacağına
vaziyetin imkân ve şeraitini düşünmeyeceksin.
Bu imkân ve şerait, çok namüsait bir mahiyette tezahür edebilir.
İstiklal ve cumhuriyetine kastedecek düşmanlar, bütün dünyada emsali görülmemiş bir galibiyetin mümessili
olabilirler.
Cebren ve hile ile aziz vatanın bütün kaleleri zapt edilmiş, bütün tersanelerine girilmiş, bütün orduları
dağıtılmış ve memleketin her kösesi bilfil işgal edilmiş olabilir.
Bütün bu şeraidden daha elim ve daha vahim olmak üzere, memleketin dâhilinde iktidara sahip olanlar, gafl
et ve dalalet ve hatta hiyanet içinde bulunabilirler.
Hatta bu iktidar sahipleri, sahibi menfaatlerini müstevlilerin siyasi emelleriyle tevhit edebilirler.
Millet, fakruzaruret içinde harap ve bitap düşmüş olabilir.
Ey Türk istikbalinin evladı!
```

İşte, bu ahval ve şerait içinde dahi vazifen, Türk istiklal ve cumhuriyetini kurtarmaktır.

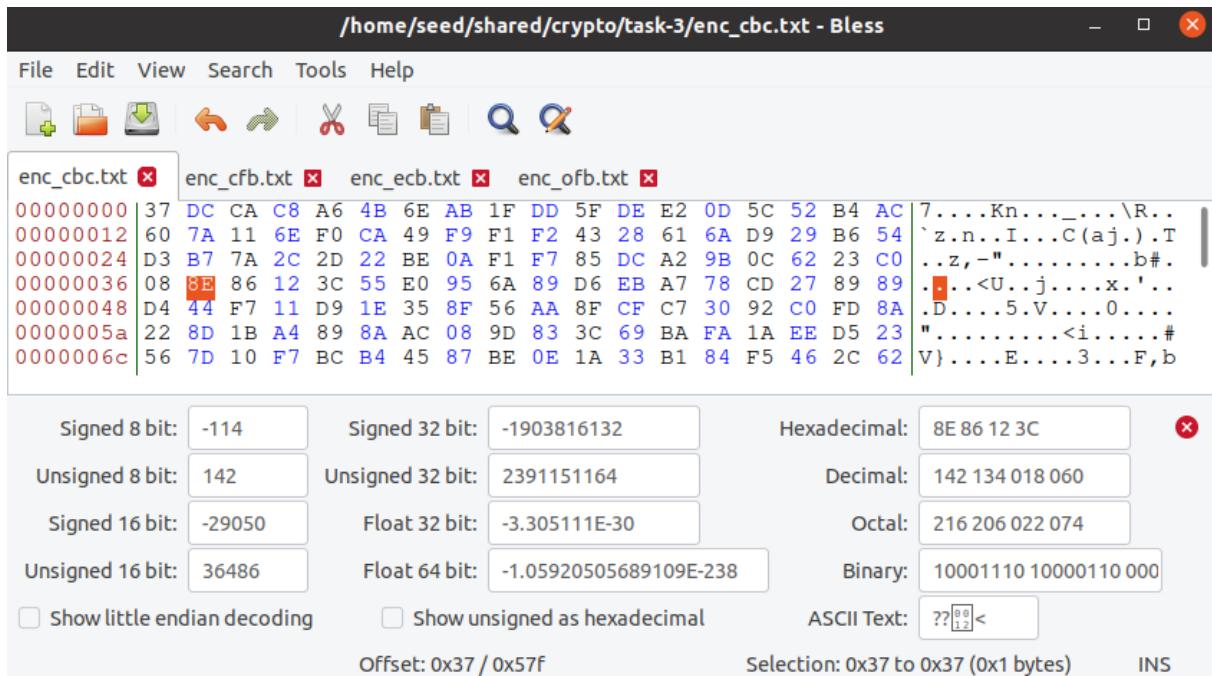
Muhtaç olduğun kudret, damarlarındaki asıl kanda mevcuttur.

```
[06/25/22] seed@VM:~/task-3$
```

- I encrypted this file using AES 128-bit block ciphers with ECB, CBC, CFB and OFB.

```
[06/25/22] seed@VM:~/task-3$ openssl enc -aes-128-ecb -in myfile.txt -out enc_ecb.txt
-K 00112233445566778899aabcccddeeff
[06/25/22] seed@VM:~/task-3$ openssl enc -aes-128-cbc -in myfile.txt -out enc_cbc.txt
-K 00112233445566778899aabcccddeeff -iv aabbccddeeff12345678912345678900
[06/25/22] seed@VM:~/task-3$ openssl enc -aes-128-cfb -in myfile.txt -out enc_cfb.txt
-K 00112233445566778899aabcccddeeff -iv aabbccddeeff12345678912345678900
[06/25/22] seed@VM:~/task-3$ openssl enc -aes-128-ofb -in myfile.txt -out enc_ofb.txt
-K 00112233445566778899aabcccddeeff -iv aabbccddeeff12345678912345678900
```

- **With Bless, I changed a bit on 55th byte of all encrypted txt files. For example in image below, selected byte (55th) was 8D. It corrupted to 8E. I saved all changes.**



- **After corrupting, I decrypted all corrupted files with same keys and IVs.**

```
[06/25/22] seed@VM:~/.../task-3$ openssl aes-128-ecb -d -in enc_ecb.txt -out dec_ecb.txt
-K 00112233445566778899aabcccddeeff
[06/25/22] seed@VM:~/.../task-3$ openssl aes-128-cbc -d -in enc_cbc.txt -out dec_cbc.txt
-K 00112233445566778899aabcccddeeff -iv aabbccddeeff12345678912345678900
[06/25/22] seed@VM:~/.../task-3$ openssl aes-128-cfb -d -in enc_cfb.txt -out dec_cfb.txt
-K 00112233445566778899aabcccddeeff -iv aabbccddeeff12345678912345678900
[06/25/22] seed@VM:~/.../task-3$ openssl aes-128-ofb -d -in enc_ofb.txt -out dec_ofb.txt
-K 00112233445566778899aabcccddeeff -iv aabbccddeeff12345678912345678900
```

- **Errors (highlighted parts)**

My assumption was correct. The most data recovery is in OFB mode. In CBC and CFB modes, more data have been lost.

- o **ECB (little part in i'th block)**

00000000	45 79 20 54 C3 BC 72 6B 20 67 65 6E C3 A7 6C 69 C4 9F	Ey T..rk gen..li...
00000012	69 21 20 0A 42 69 72 69 6E 63 69 20 76 61 7A 69 66 65	i! .Birinci vazife
00000024	6E 3B 20 54 C3 BC 72 6B 20 69 73 74 D/ EB 41 36 99 51	n; T..rk ist..A6.Q
00000036	E4 4B F6 DE 4D 6C DC 6C 63 B0 63 75 6D 68 75 72 69 79	.K..Ml.lc.cumhuriy
00000048	65 74 69 6E 69 2C 20 69 6C 65 6C 65 62 65 74 20 6D 75	etini, illelebet mu
0000005a	68 61 66 61 7A 61 20 76 65 20 6D C3 BC 64 61 66 61 61	hafaza ve m..dafaa
0000006c	20 65 74 6D 65 6B 74 69 72 2E 0A 4D 65 76 63 75 64 69	etmektir..Mevcudi
0000007e	79 65 74 69 6E 69 20 76 65 20 69 73 74 69 6B 62 61	yetinin ve istikba
00000090	6C 69 6E 69 6E 20 79 65 67 C3 A2 6E 65 20 74 65 6D 65	linin yeg..ne teme
000000a2	6C 69 20 62 75 64 75 72 2E 0A 42 75 20 74 65 6D 65 6C	li budur..Bu temel
000000b4	2C 20 73 65 6E 69 6E 20 65 6E 20 6B C4 B1 79 6D 65 74	, senin en k..ymet
000000c6	6C 69 20 68 61 7A 69 6E 65 6E 64 69 72 2E 0A C4 B0 73	li hazinendir....s
000000d8	74 69 6B 62 61 6C 64 65 20 64 61 68 69 20 73 65 6E 69	tikbalde dahi seni
000000ea	20 62 75 20 68 61 7A 69 6E 65 64 65 6E 20 6D 61 68 72	bu hazineden mahr
000000cf	75 6D 20 65 74 6D 65 6B 20 69 73 74 65 79 65 63 65 6B	um etmek isteyecek
0000010e	20 64 C3 A2 68 69 6C C3 AE 20 76 65 20 68 61 72 69 63	d..hil.. ve haric
00000120	C3 AE 20 62 65 64 68 61 68 6C 61 72 C4 B1 6E 20 6F 6C	.. bedhahlar..n ol
00000132	61 63 61 6B 74 C4 B1 72 2E 0A 42 69 72 20 67 C3 BC 6E	acakt..r..Bir g..n

- CBC (i and i+1'th blocks)

000000000	45 79 20 54 C3 BC 72 6B 20 67 65 6E C3 A7 6C 69 C4 9F	Ey T..rk gen..li..
000000012	69 21 20 0A 42 69 72 69 6E 63 69 20 76 61 7A 69 66 65	i! .Birinci vazife
000000024	6E 3B 20 54 C3 BC 72 6B 20 69 73 74 F6 D5 61 72 DE 5B	n; T..rk ist..ar.[
000000036	E9 12 3C 14 30 F9 7C 61 97 17 63 75 6D 68 75 72 69 7A ..<.0. a..cumhuriz	etini, ilelebet mu
000000048	65 74 69 6E 69 2C 20 69 6C 65 6C 65 62 65 74 20 6D 75	hafaza ve m..dafa
00000005a	68 61 66 61 7A 61 20 76 65 20 6D C3 BC 64 61 66 61 61	etmektir..Mevcudi
00000006c	20 65 74 6D 65 6B 74 69 72 2E 0A 4D 65 76 63 75 64 69	yetinin ve istikba
00000007e	79 65 74 69 6E 69 20 76 65 20 69 73 74 69 6B 62 61	linin yeg..ne teme
000000090	6C 69 6E 69 6E 20 79 65 67 C3 A2 6E 65 20 74 65 6D 65	li budur..Bu temel
0000000a2	6C 69 20 68 61 7A 69 6E 65 6E 64 69 72 2E 0A C4 B0 73	, senin en k..ymet
0000000b4	2C 20 73 65 6E 69 6E 20 65 6E 20 6B C4 B1 79 6D 65 74	li hazinendir....s
0000000c6	6C 69 20 68 61 7A 69 6E 65 6E 64 69 72 2E 0A C4 B0 73	tikbalde dahi seni
0000000d8	74 69 6B 62 61 6C 64 65 20 64 61 68 69 20 73 65 6E 69	bu hazineden mahr
0000000ea	20 62 75 20 68 61 7A 69 6E 65 64 65 6E 20 6D 61 68 72	um etmek isteyecek
0000000cf	75 6D 20 65 74 6D 65 6B 20 69 73 74 65 79 65 63 65 6B	d..hil.. ve haric
00000010e	20 64 C3 A2 68 69 6C C3 AE 20 76 65 20 68 61 72 69 63	.. bedhahlar..n ol
000000120	C3 AE 20 62 65 64 68 61 68 6C 61 72 C4 B1 6E 20 6F 6C	acakt..r..Bir g..n
000000132	61 63 61 6B 74 C4 B1 72 2E 0A 42 69 72 20 67 C3 BC 6E	

- CFB (i and i+1'th blocks)

000000000	45 79 20 54 C3 BC 72 6B 20 67 65 6E C3 A7 6C 69 C4 9F	Ey T..rk gen..li..
000000012	69 21 20 0A 42 69 72 69 6E 63 69 20 76 61 7A 69 66 65	i! .Birinci vazife
000000024	6E 3B 20 54 C3 BC 72 6B 20 69 73 74 6B 6C 61 6C 69	n; T..rk istiklali
000000036	6E 68 2C 20 54 C3 BC 72 6B 20 C9 93 76 40 A2 80 1D 24	nh, T..rk ...v@...\$
000000048	4D 51 A0 ED A2 19 62 81 6C 65 6C 65 62 65 74 20 6D 75	MQ....b.ilelebet mu
00000005a	68 61 66 61 7A 61 20 76 65 20 6D C3 BC 64 61 66 61 61	hafaza ve m..dafa
00000006c	20 65 74 6D 65 6B 74 69 72 2E 0A 4D 65 76 63 75 64 69	etmektir..Mevcudi
00000007e	79 65 74 69 6E 69 20 76 65 20 69 73 74 69 6B 62 61	yetinin ve istikba
000000090	6C 69 6E 69 6E 20 79 65 67 C3 A2 6E 65 20 74 65 6D 65	linin yeg..ne teme
0000000a2	6C 69 20 62 75 64 75 72 2E 0A 42 75 20 74 65 6D 65 6C	li budur..Bu temel
0000000b4	2C 20 73 65 6E 69 6E 20 65 6E 20 6B C4 B1 79 6D 65 74	, senin en k..ymet
0000000c6	6C 69 20 68 61 7A 69 6E 65 6E 64 69 72 2E 0A C4 B0 73	li hazinendir....s
0000000d8	74 69 6B 62 61 6C 64 65 20 64 61 68 69 20 73 65 6E 69	tikbalde dahi seni
0000000ea	20 62 75 20 68 61 7A 69 6E 65 64 65 6E 20 6D 61 68 72	bu hazineden mahr
0000000cf	75 6D 20 65 74 6D 65 6B 20 69 73 74 65 79 65 63 65 6B	um etmek isteyecek
00000010e	20 64 C3 A2 68 69 6C C3 AE 20 76 65 20 68 61 72 69 63	d..hil.. ve haric
000000120	C3 AE 20 62 65 64 68 61 68 6C 61 72 C4 B1 6E 20 6F 6C	.. bedhahlar..n ol
000000132	61 63 61 6B 74 C4 B1 72 2E 0A 42 69 72 20 67 C3 BC 6E	acakt..r..Bir g..n

- OFB (only one bit in i'th block)

000000000	45 79 20 54 C3 BC 72 6B 20 67 65 6E C3 A7 6C 69 C4 9F	Ey T..rk gen..li..
000000012	69 21 20 0A 42 69 72 69 6E 63 69 20 76 61 7A 69 66 65	i! .Birinci vazife
000000024	6E 3B 20 54 C3 BC 72 6B 20 69 73 74 6B 6C 61 6C 69	n; T..rk istiklali
000000036	6E 6A 2C 20 54 C3 BC 72 6B 20 69 73 74 6B 6C 61 6C 69	n, T..rk cumhuriy
000000048	65 74 69 6E 69 2C 20 69 6C 65 6C 65 62 65 74 20 6D 75	etini, ilelebet mu
00000005a	68 61 66 61 7A 61 20 76 65 20 6D C3 BC 64 61 66 61 61	hafaza ve m..dafa
00000006c	20 65 74 6D 65 6B 74 69 72 2E 0A 4D 65 76 63 75 64 69	etmektir..Mevcudi
00000007e	79 65 74 69 6E 69 20 76 65 20 69 73 74 69 6B 62 61	yetinin ve istikba
000000090	6C 69 6E 69 6E 20 79 65 67 C3 A2 6E 65 20 74 65 6D 65	linin yeg..ne teme
0000000a2	6C 69 20 62 75 64 75 72 2E 0A 42 75 20 74 65 6D 65 6C	li budur..Bu temel
0000000b4	2C 20 73 65 6E 69 6E 20 65 6E 20 6B C4 B1 79 6D 65 74	, senin en k..ymet
0000000c6	6C 69 20 68 61 7A 69 6E 65 6E 64 69 72 2E 0A C4 B0 73	li hazinendir....s
0000000d8	74 69 6B 62 61 6C 64 65 20 64 61 68 69 20 73 65 6E 69	tikbalde dahi seni
0000000ea	20 62 75 20 68 61 7A 69 6E 65 64 65 6E 20 6D 61 68 72	bu hazineden mahr
0000000cf	75 6D 20 65 74 6D 65 6B 20 69 73 74 65 79 65 63 65 6B	um etmek isteyecek
00000010e	20 64 C3 A2 68 69 6C C3 AE 20 76 65 20 68 61 72 69 63	d..hil.. ve haric
000000120	C3 AE 20 62 65 64 68 61 68 6C 61 72 C4 B1 6E 20 6F 6C	.. bedhahlar..n ol
000000132	61 63 61 6B 74 C4 B1 72 2E 0A 42 69 72 20 67 C3 BC 6E	acakt..r..Bir g..n