Advanced Encryption Standard

(a) Folosind cheia de criptare de 128 de biți:

```
AB 89 CD 01 EF 23 AB 45 CD 01 AB 23 CD 45 EF 67
```

Criptați mesajul:

```
Advanced Encryption Standard
```

Rezultat:

```
BA 95 BF 9E 2F E4 D8 69 E4 33 EB EE 22 21 FF 50 03 0D 8A B4 63
B3 37 DE 4F D7 37 FC 98 5E C1 9E
```

(b) Folosind cheia de la punctul anterior și padding mode 1–0 decriptați mesajul:

```
14 5F 5D 4C F4 B9 20 0F 7E BD 56 53 19 96 9A 1B 5A 08 75 29 08
18 4E 79 13 7C B7 F6 12 9A 93 D4
```

Întrucât mesajul este deja pe 32 de bytes, acesta nu mai are nevoie de padding.
Folosesc CBC cu IV:

```
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Rezultat:

```
Joan Daemen ; Vincent Rijmen
```

(c) Se consideră următoarea intrare într-o rundă AES:

04	07	E2	49
F2	78	2F	C5
CA	28	01	D7
97	45	96	10

și cheia de rundă. Care este ieșirea din rundă?

Aplic, pe rând, cei 4 pași: Sub Bytes, Shift Rows, Mix Columns și Add Round Key.

1. Sub Bytes:

Înlocuiesc valorile din tabel cu echivalentul lor din acest tabel. Pentru a găsi valoarea echivalentă, caut prima cifră a numărului din tabelul de intrare pe linie, a doua cifră pe coloană și intersectez cele 2 componente. Tabelul este cunoscut:

		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
	1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
	2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
	3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
	4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
	5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
	6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
	7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
	8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
	9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
	a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
	b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
	c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
	d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
	e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
	f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

Tabelul devine:

30	38	3B	A4
04	C1	4E	07
10	EE	09	0D
85	68	35	7C

2. Shift Rows:

Permut fiecare linie la stânga de indicele liniei -1 ori (prima linie niciodată, a doua o dată, a treia de două ori, a patra de trei ori):

30	38	3B	A4
C1	4E	07	04
09	0D	10	EE
7C	85	68	35

3. Mix Columns:

Înmulțesc fiecare coloană cu matricea cunoscută de mai jos și înlocuiesc valorile.*

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

Înmulțirea nu este una clasică. Algoritmul este explicat aici: https://www.angelfire.com/biz7/atleast/mix_columns.pdf.

Matricea nou obținută:

4D	12	1B	84
CE	06	6D	B0
67	F8	A4	F8
A0	FA	76	77

4. Add Round Key:

Xorez fiecare valoare cu echivalenta sa de pe aceeași poziție din cheia de rundă dată la început:

21	35	AC	6C
75	50	AF	1B
17	62	6B	F0
87	0B	3C	9B

Ieșirea din rundă va fi:

6C	27	B7	E8
BB	56	C2	AB
70	9A	CF	08
27	F1	4A	EC

* Calculele de la pasul 3:

{30 . 02} + {C1 . 03} + {09 . 01} + {7C . 01}
= 60 ^ {1100 0001 . 11 (in binar)} ^ 09 ^ 7C
= 60 ^ {1100 0001 . 10} ^ {1100 0001 . 01} ^ 09 ^ 7C
= 60 ^ {1100 0001 . 10} ^ C1 ^ 09 ^ 7C
= 60 ^ {1100 0001 << 1 (pe 8 biti)} ^ C1 ^ 09 ^ 7C
= 60 ^ {1000 0010 ^ 0001 1011} ^ C1 ^ 09 ^ 7C
= 60 ^ 99 ^ C1 ^ 09 ^ 7C
= 4D

{30 . 01} + {C1 . 02} + {09 . 03} + {7C . 01}
= 30 ^ {1000 0010 ^ 0001 1011} ^ 1B ^ 7C
= 30 ^ 99 ^ 1B ^ 7C
= CE

{30 . 01} + {C1 . 01} + {09 . 02} + {7C . 03} = 30 ^ C1 ^ 12 ^ F8 ^ 7C = 67
{30 . 03} + {C1 . 01} + {09 . 01} + {7C . 02} = 90 ^ C1 ^ 09 ^ F8 = A0

{38 . 02} + {4E . 03} + {0D . 01} + {85 . 01} = 70 ^ EA ^ 0D ^ 85 = 12
{38 . 01} + {4E . 02} + {0D . 03} + {85 . 01} = 38 ^ 9C ^ 27 ^ 85 = 06

{38 . 01} + {4E . 01} + {0D . 02} + {85 . 03}
= 38 ^ 4E ^ 1A ^ {0000 1010 ^ 0001 1011} ^ 85
= 38 ^ 4E ^ 1A ^ 11 ^ 85
= F8

{38 . 03} + {4E . 01} + {0D . 01} + {85 . 02}
= A8 ^ 4E ^ 0D ^ {0000 1010 ^ 0001 1011}
= A8 ^ 4E ^ 0D ^ 11
= FA

{3B . 02} + {07 . 03} + {10 . 01} + {68 . 01} = 76 ^ 15 ^ 10 ^ 68 = 1B
{3B . 01} + {07 . 02} + {10 . 03} + {68 . 01} = 3B ^ 0E ^ 30 ^ 68 = 6D
{3B . 01} + {07 . 01} + {10 . 02} + {68 . 03} = 3B ^ 07 ^ 20 ^ D0 ^ 68 = A4
{3B . 03} + {07 . 01} + {10 . 01} + {68 . 02} = B1 ^ 07 ^ 10 ^ D0 = 76

{A4 . 02} + {04 . 03} + {EE . 01} + {35 . 01}
= {0100 1000 ^ 0001 1011} ^ 0C ^ EE ^ 35
= 53 ^ 0C ^ EE ^ 35
= 84

{A4 . 01} + {04 . 02} + {EE . 03} + {35 . 01}
= A4 ^ 08 ^ {1101 1100 ^ 0001 1011} ^ EE ^ 35

= A4 ^ 08 ^ C7 ^ EE ^ 35

= B0

{A4 . 01} + {04 . 01} + {EE . 02} + {35 . 03}

= A4 ^ 04 ^ {1101 1100 ^ 0001 1011} ^ 9F

= A4 ^ 04 ^ C7 ^ 9F

= F8

{A4 . 03} + {04 . 01} + {EE . 01} + {35 . 02}

= {0100 1000 ^ 0001 1011} ^ A4 ^ 04 ^ EE ^ 6A

= 53 ^ A4 ^ 04 ^ EE ^ 6A

= 77