Criptografie
tema - 1

1.

a) „The Da Vinci Code" - Dan Brown

b) „The Imitation Game" - Andrew Hodges

c) „Between Silk and Cyanide" - Leo Marks.

2. $A = (101000110101)_2$, $B = (100001111011)_2$

Pasul 1: A - B

```
  101000110101 -
  100001111011
  ------------
  000110111010
```

Pasul 2: B - (A - B)

```
  100001111011 -
  000110111010
  ------------
  011011000001
```

Pasul 3:

```
  011011000001 -
  000110111010
  ------------
  010100000111
```

Pasul 4:

```
  010100000111 -
  000110111010
  ------------
  001101001101
```

Pasul 5:

```
  001101001101 -
  000110010011
  ------------
  000110010011
```

Pasul 6

```
  000110111010 -
  000110010011
  ------------
  000 000100111
```

Pasul 7

```
  000110010011 -
  000000100111
  ------------
  000101101100
```

Pasul 8

```
  000101101100 -
  000000100111
  ------------
  000101000101
```

Pasul 9

```
  000101000101 -
  000000100111
  ------------
  000100011110
```

Pasul 10

```
  000100011110 -
  000000100111
  ------------
  000011111111
```

Pasul 11

```
  000011111111 -
  000000100111
  ------------
  000011011000
```

Pasul 12

```
  000011011000 -
  000000100111
  ------------
  000010110001
```

Pasul 13

```
  000010110001
  000000100111
  ------------
  000010001010.
```

Pasul 14

0000100001010 -
0000000100111
0000011000011

Pasul 15

0000001100011 -
0000000100111
0000001000100

Pasul 16

0000001000100
0000000100111
0000000011101

encode $= (1101)_2$

$1101_2 = 13_{10}$ $\quad 2^3 + 2^2 + 1 = 13$

3 2 1

(3)

Numarul de pasi depinde de câte ori putem împărți numărul N la b pasi și la o

Nr de pasi $\approx \log_b(N)$

Dacă N este repr cu k biți, atunci aprox $N \approx 2^k$, deci

$\log_b(N) \approx \log_b(2^k) = k \cdot \log_b(2)$

=> Complexitate $O(k)$

(5) a) $100100_2 = (?)_{10}$

5 4 3 2 1 0

$100100 = 1 \cdot 2^5 + 1 \cdot 2^2 = 32 + 4 = 36$

b) $(2F)_{16} = (?)_{10}$

$2F = 2 \cdot 16 + 15 \cdot 1 = 32 + 15 = 47$

c) $331_6 = ?_4$

$331 = 3 \cdot 6^2 + 3 \cdot 6 + 1 = 3 \cdot 36 + 3 \cdot 6 + 1 = 108 + 18 + 1 = 127$

127	4
12	
7	31
4	
$\boxed{3}$	

31	4
28	
$\boxed{3}$	7

7	4
4	
$\boxed{3}$	1

1
$\boxed{1}$

1333_4

d) $2 \cdot 13 = 26_3$ $\quad$ 26 : 13 = 2

(6) $12^{60} \pmod{77} = (12^2)^{30} = (144)^{30} = (67^2)^{15} = 4489(4489)^{14}$

$= 23(23^2)^7 = 23(67)^7 = \underbrace{23\cdot 67}_{1}(67^2)^3 = (23)^3 = 23(23^2) = 23\cdot 67 = 1$