ex6. Alice utilizează un criptosistem Merkle-Hellman pe un alfabet cu 26 caractere (A-Z) unitățile de mesaj având un caracter. Cheia publică a lui Alice este șirul { 8, 24, 3, 14, 57 } iar cheia secretă este ($b=23$, $m=61$). Bob dorește să-i trimită lui Alice mesajul HELLO. Criptați mesajul

$H = 7 \to 00111 = 1\cdot8 + 1\cdot23 + 1\cdot3 + 0\cdot14 + 0\cdot57 = 34$

$E = 4 \to 00100 = 0\cdot8 + 0\cdot24 + 1\cdot3 + 0\cdot14 + 0\cdot57 = 3$

$L = 11 \to 01011 = 1\cdot8 + 1\cdot24 + 0\cdot3 + 1\cdot14 + 0\cdot57 = 46$

$L = 11 \to 01011 = - " - = 46$

$O = 14 \to 01000 = 0\cdot8 + 0\cdot24 + 0\cdot3 + 1\cdot14 + 0\cdot57 = 57.$

ex1 Pentru fiecare dintre șirurile următoare decideți dacă este supercrescător și det. toate soluțiile problemei rucsacului cu volumul corespunzător.

a) $(2, 3, 7, 20, 35, 69)$, $V = 45$.

$2 + 3 = 5 < 7$

$5 + 7 = 12 < 20$

$12 + 20 = 32 < 35$

$32 + 35 = 67 < 69$ → șirul este supercrescător.

$V = 3 + 7 + 35 = 45.$

b) $(1, 2, 5, 9, 20, 49)$, $V = 73$

$1 + 2 = 3 < 5$

$3 + 5 = 8 < 9$

~~$V = 49 + 5 + 2 \cdot 9 + 1 = 73$~~

$8 + 9 = 17 < 20$

$17 + 20 = 37 < 49$ ⇒ șir supercrescător

c) $(1, 3, 7, 12, 22, 45)$, $V=67$

$1+3=4<7$

$4+7=11<12$

$11+12=23>22$ → șirul nu este supercrescator.

~~$V=3\cdot 22+1\cdot 1=67$~~

d) $(2, 3, 6, 11, 21, 40)$ $V=39$.

$2+3=5<6$

$5+6=11$ => nu e șir supercrescator.

~~$V=3\cdot 11+1\cdot 6.=39$~~

e) $(4, 5, 10, 30, 50, 101)$, $V=186$.

$4+5=9<10$

$9+10=19<30$

$19+30=49<50$

$49+50=99<101$ → șir supercrescator.

$V=101+50+30+5=186$

f) $(3, 5, 8, 15, 28, 60)$ $V=43$.

$3+5=8=8$ => șirul nu e supercrescator.

2) Decriptați următorul text cifrat obținut folosind criptosistemul lui Cezar.

HWDUYTLWFUMD

$K=5$

	H	W	D	U	Y	T	L	W	F	U	M	D
C	7	22	3	20	24	19	11	22	5	20	12	3
m(mod 26)	2	17	24	15	19	14	6	17	0	15	7	24
M	C	R	Y	P	T	O	G	R	A	P	H	Y

ex 4) Fie matricea de criptare $A=\begin{pmatrix}2&3\\7&8\end{pmatrix}\in \mathcal{M}_{2\times2}(\mathbb{Z}_{26})$

Det. matricea de decriptare și decriptați

FWMDiQ

$$\det A = 2\cdot8-3\cdot7=16-21=-5=21$$

$$(\det A)^{-1}=(-5)^{-1}=5$$

$$A^{-1}=(\det A)^{-1}\begin{pmatrix}d&-b\\-c&a\end{pmatrix}=5\cdot\begin{pmatrix}8&-3\\-7&2\end{pmatrix}=\begin{pmatrix}40&-15\\-35&10\end{pmatrix}$$

$$=\begin{pmatrix}14&11\\17&10\end{pmatrix}$$

$$\begin{pmatrix}14&11\\17&10\end{pmatrix}\begin{pmatrix}F&M&i\\W&D&Q\end{pmatrix}=\begin{pmatrix}14&11\\17&10\end{pmatrix}\begin{pmatrix}5&12&8\\22&3&16\end{pmatrix}$$

$$=\begin{pmatrix}5\cdot14+11\cdot22 & 14\cdot12+3\cdot11 & 14\cdot8+11\cdot16\\17\cdot5+10\cdot22 & 17\cdot12+3\cdot10 & 17\cdot8+10\cdot16\end{pmatrix}$$

$$= \begin{pmatrix} 18+8 & 12+7 & 8+20 \\ 7+12 & 22+4 & 6+4 \end{pmatrix} = \begin{pmatrix} 0 & 19 & 2 \\ 19 & 0 & 10 \end{pmatrix}$$

$$= \begin{pmatrix} A & T & C \\ T & A & K \end{pmatrix}$$

Textul decriptat este: ATTACK.

5) Verificați cu ajutorul algoritmului Fermat dacă numărul 52997 este prim sau compus.

$$2^{52996} = 4^{26498} = 16^{13249} = 16 \cdot 256^{6624}$$

$$= 16 \cdot (256^2)^{3312} = 16 \cdot (12539^2)^{1656} = 16 \cdot (37419^2)^{828}$$

$$= 16 \cdot (821)^{418} = 16 \cdot (821^2)^{207} = 16 \cdot 38077 (38077^2)^{103}$$

$$= 26265 \cdot 19000 \cdot (19000^2)^{51} = 15248 \cdot 37433 (37433^2)^{25}$$

$$= 694 \cdot 41806 \cdot (41806^2)^{12} = 24005 \cdot (65702)^6 = \cancel{240}$$

$$= 24005 (25342^2)^3 = 24005 \cdot 52315 \cdot 52315^2$$

$$= 4663 \cdot 41148 = 23984 \pmod{52997} \rightarrow$$

52997 compus.

7) Criptați următorul text, folosind criptosistemul lui Vigenere cu cheia CHEIE pe un alfabet cu 28 caractere (A - Z _ ?) :

CE_ALGORITM_STA_LA_BAZA_CRIPTOSISTEMULUI_DES?

CE_ALGORITM_STA_LA_BAZA_CRIPTOSISTEMULUI_DES?

CHEIECHEIECHEIECHEIECHEIECHEIECHEIECHEIECHEIE

m	E	L	C	i	P	i	V	V	Q	X	O	F	W	?	E
m	4	11	2	8	15	8	21	21	16	23	14	5	22	27	4
K	C	H	E	i	E	C	H	E	i	E	C	H	E	i	E
K	2	7	4	8	4	2	7	4	8	4	2	7	4	8	4
c mod30	2	4	26	0	11	6	14	17	8	19	12	26	18	19	0
C	C	E	-	A	L	G	O	R	i	T	M	8	S	T	A

G	m	G	T	P	T	?	S	U	P	W	?	i	O	?	P	A	M	A	K	i	_	A	S	E	G	O	M	E	E
6	m	6	19	15	19	27	18	20	15	22	27	8	14	27	15	0	12	0	10	8	26	0	18	4	6	14	12	4	4
i	K	E	C	H	E	İ	E	C	H	E	i	E	C	H	E	i	E	C	H	E	i	C	H	E	i	E	C	H	E
8	K	4	2	7	4	8	4	2	7	4	8	4	2	7	4	8	4	2	7	4	8	2	7	4	0	4	2	7	4
26	c mod30	2	17	8	15	19	14	18	8	18	19	4	12	20	11	20	8	26	3	4	18	26	11	0	26	10	25	0	
	C	C	R	i	P	T	O	S	i	S	T	E	M	U	L	U	i	_	D	E	S	_	L	A	_	B	A	Z	A

RASPUNS:

ELCiPiVVQXOFW?EASEGOMEEGGTPT?SUPW?iO?PAMAKi_ ex 8) Decriptați mesajul

MBPXMFUFPBWO

Știind că a fost cifrat cu criptosistemul Vegniere pe un alfabet cu 26 caractere (A - Z) și că mesajul în clar, se încheie cu semnatura PAUL.

m	M	B	P	X	M	F	U	F	P	B	W	O
m	12	1	15	23	12	5	20	5	15	1	22	14
K	A	B	C	D	A	B	C	D	A	B	C	D
K	0	1	2	3	0	1	2	3	0	1	2	3
C(mod30)	12	0	13	20	12	4	18	2	15	0	20	11
C	M	A	N	U	M	E	S	C	P	A	U	L

ex 9) Găsiți factorii primi ai numărului 15347.

$\sqrt{1.53.47}$ | 123

1 | $23 \cdot \underline{2} = 44$

$=53$ | $24\underline{3} \cdot \underline{3} = 729$

44

$=347$

729

Deci $[\sqrt{15347}] = 123$.

$t = 124. \Rightarrow t^2 - n = 15376 - 15347 = 29$

$t = 125 \rightarrow t^2 - n = 15625 - 15347 = 278 = 2 \cdot 139$

$t = 126 \rightarrow 15.876 - 15347 = 529. = 23^2$

Deci, $(126^2 - 15347) = 23^2$.

$126^2 = 23^2 \pmod{15347}$

$126^2 - 23^2 \vdots 15347$

$(126-23)(126+23) \vdots 15347$

$(103, 15347)\cdot(149, 15347) = 15347.$

Așadar, $103 \cdot 149 = 15347.$

ex 10) Alice și Bob doresc să comunice folosind Criptosistemul RSA. Alice alege nr. prime $p=7, q=11$ pt. a-și determina cheile de criptare / decriptare și alege exponentul de decriptare $d>1$ minimul posibil

a) Aflați cheia de criptare (n, e) a lui Alice

b) Bob îi transmite lui Alice mesajul: B!BTBL.

Știind că lungimea blocurilor la citire este 1 și la scriere este 2, decriptați textul.

a) $n = 7 \cdot 11 = 77.$

$(p-1)(q-1) = f(n)$

$6 \cdot 10 = f(n) \Rightarrow f(n) = 60.$

$d_A \cdot e_A \equiv 1 \pmod{f(n)}$

$d_A \cdot e_A \equiv 1 \pmod{60}$

$d_A \in \{3, 4, \dots, f(n)-1\}$

$\in \{3, 4, \dots, 59\}$

$(\varphi(n), e_A) = 1 \Rightarrow (60, e_A) = 1,\ e \geq 3,\ e \leq 59 \Rightarrow e = 7.$

$\Rightarrow (n, e) = (60, 7)$

5) B! BTBL.

$B! = 1 \cdot 30 + 28 = 58 \Rightarrow m = 58^3 (\text{mod } 77) = (7)(1) = (2)(11) = CL$

$BT = 1 \cdot 30 + 19 = 49 \Rightarrow m = 49^3 (\text{mod } 77) = (7)(0) = (2)(10) = C4$

$BL = 1 \cdot 30 + 11 = 44 \Rightarrow m = 44^3 (\text{mod } 77) = (22 =$ W

B! BTBL =

$B! = 71 \Rightarrow m' = (71)^{60} (\text{mod } 77) = (72^2)^{30} = (25^2)^{15} = 9 \cdot (9^2)^7$

$= 9 \cdot 4 \cdot (4^2)^3 = 36 \cdot 16 \cdot \underset{25}{16^2} = 37 \cdot 25 = 1 = B$

$BT = 70 \Rightarrow m' = (70)^{60} (\text{mod } 77) = (70^2)^{30} = (49^2)^{15} = 14(14^2)^7$

~~$= 14 \cdot 49 \cdot (49^2)^3$~~ $= 14 \cdot 49 \cdot 14 \cdot 14^2$

$= 14 \cdot 42 \cdot (42^2)^3 = 49 \cdot 70 \cdot 70^2 = 42 \cdot 49 = 56$

$BL = (22)^{60} = 22 = W$

ex11) Alice utilizează un criptosistem El Gamal și are cheia publică (31, 3, 19). Bob dorește să-i transmită mesajul X și alege parametrul k=3. Să se determine mesajul criptat. Alfabetul folosit are 30 de caractere, în care literele A-Z au echivalenți numerici 0-25, = 26, ? = 27, ! = 28 și . = 29.

$m = X = 23$

$k = 3$

$p = 31$

$g = 3$

$\alpha = 19$

$K_e = (31, 3, 19)$

$u = g^k \pmod p$

$v = m \cdot \alpha^k \pmod p$

$u = 3^3 \pmod{31} \equiv 27 \pmod{31}$

$v = 23 \cdot 19^3 \pmod{31} \equiv 23 \cdot 19 \cdot 19^2 \pmod{31}$

$\equiv 3 \cdot 20 \pmod{31} \equiv 29 \pmod{31}$

$(u, v) = (27, 29) \to (?, .)$

ex12) Alice și Bob doresc să stabilească o cheie secretă K (pe care doar ei să o cunoască folosind criptosistemul Diffie - Hellman. Ei aleg nr. prim $p = 17$ și generatorul $g = 5$ al lui Z_{17}. Alice alege exponentul secret $a=3$, iar Bob alege exponentul secret $b=6$. Det. cheia K.

$u = g^a \pmod{p} \Rightarrow u = 5^3 \pmod{17} \equiv 6$

$v = g^b \pmod{p} \Rightarrow v = 5^6 \pmod{17} \equiv 2$

- A calculează $K = v^a \pmod{p} = 2^3 \pmod{17} \equiv 8$

B calculează $K = u^b \pmod{p} = 6^6 \pmod{17} \equiv 8$

$\Rightarrow$ Cheia secretă este $K = 8$.

ex13) Alice primește mesajul (30,7), obținut cu ajutorul unui criptosistem El Gamal. Decriptați mesajul, cunoscând cheia publică a lui Alice $(p = 43, g = 3)$

- A primește (u, v)
- A ridică u la puterea $p-1-a_A$ și obține

$w = u^{p-1-a_A} = u^{-a_A} \pmod{p}$

- A calculează $m' = v \cdot w \pmod{p}$.

- $(30, 7)$.
- $w = 30^{43-1-a_A}$, $a \in (0, p-1), a \in (0, 42)$.

$w = 30^{-a_A} = 30^{-1} \pmod{p} = 30^{-1} \pmod{43} \equiv 33$

- $m' = v \cdot w \pmod{p} = 7 \cdot 33 \pmod{43} \equiv 16 \pmod{43}$

ex14) Ana şi Bob folosesc criptosistemul Elgamal. Ana are cheia privată Kd=(p=71, g=33, a=34).

a) Determinaţi cheia publică a Anei

b) Bob alege K=3 pt. a-i transmite Anei mesajul AZi. Ştiind că K se păstrează, lungimea blocurilor în clar este 1, şi a celor criptate este 2, det. mesajul criptat. Alfabetul folosit.

$$A - Z\,?\,!\,.\,1\,2\,3\,4\,5\,6\,7\,8\,\underset{37}{9}$$

$p=71,\ g=33,\ a=89.$

$$33^{34} \pmod{71} = (33^2)^{17} \equiv 24\cdot(24^2)^8 \equiv 24\cdot(8^2)^4 \equiv$$

$$= 24\cdot(64^2)^2 \equiv 24\cdot 49^2 \equiv 24\cdot 58 \equiv 43 \pmod{71}$$

Cheia publică a Anei: $(71, 33, 43)$

b) $u = g^k \pmod{p} = 33^3 \pmod{71} \equiv 33\cdot 33^2 \pmod{71} \equiv 33\cdot 24 \equiv 11 \pmod{71}$

AZi -> 0258

$v = 258 \cdot 34 \pmod{71} \equiv 35 \pmod{71}$

ex 15) Pentru un număr natural K determinați un şir supercrescător $\{a_0, a_1, \dots, a_{k-1}\}$ a. î. numerele naturale $a_0, a_1, \dots, a_{k-1}$ sunt minime. Rezolvați problema rucsacului pentru acest şir şi $V = 473$.

$\{v_0, \dots, v_{k-1}\}$ - şir supercrescător dacă

$$v_i > \sum_{j=0}^{i-1} v_j \,, \forall i \in \overline{1,k-1}$$

pt. a obține un şir supercrescător a.î. $a_0, \dots, a_{k-1}$ să fie minime, începem de la $a_0 = 1$ şi calculăm restul valorilor ca $a_i = \sum_{j=0}^{i-1} a_j + 1, \ \forall i \in \overline{1,k-1}$

Pentru a rezolva pb. rucsacului pt. $V = 473$ obț. acest şir:

$k = 1 \Rightarrow$ suma $= 1$.

$k = 2 \Rightarrow$ suma $= 2$ (2)

$k = 3 \Rightarrow$ sum $= 6$ $(1, 2, 4)$

$k = 4 \Rightarrow$ suma $= 14$ $(2, 4, 8)$

$k = 5 \Rightarrow$ suma $= 30$

$k = 6 \Rightarrow$ suma $= 62$.

$k = 7 \Rightarrow$ suma $= 126$.

$k = 8 \Rightarrow$ suma $= 256$

$k = 9 \Rightarrow$ suma $= 510$ $\Rightarrow$ şirul: $(1, 2, 4, 8, 16, 32, 64, 168, 256)$

- $V = 473$

  $\rightarrow 473 - \boxed{256} = 217$

- $V = 217 - \boxed{128} = 89$

- $V = 89$

  $\rightarrow 89 - \boxed{64} = 25.$

- $V = 25 \rightarrow 25 - \boxed{16} = 9$

- $V = 9 \rightarrow 9 - \boxed{8} = 1.$

- $V = 1 \rightarrow 1 - \boxed{1} = 0.$

Valorile ~~sunt~~ selectate sunt: $\{256, 128, 64, 16, 8, 1\}$.

<u>ex 3</u>. Alice utilizează un criptosistem Markle-Hellman pe un alfabet cu 26 de caractere (A-Z), unitățile de mesaj având un caracter. Cheia publică a lui Alice este șirul {34, 51, 58, 11, 39}, iar cheia secretă este (b=18, m=61). Criptați mesajul "WHY" și apoi decriptați-l:

Criptarea:

$$W = 22 \to \underline{1}\,\underline{0}\,\underline{1}\,\underline{1}\,\underline{0} \Rightarrow c_1 = 0\cdot 34 + 1\cdot 51 + 1\cdot 58 + 0\cdot 11 + 1\cdot 39 = 148.$$

$$H = 7 \to \underline{0}\,\underline{0}\,\underline{1}\,\underline{1}\,\underline{1} \Rightarrow c_2 = 134 + 1\cdot 51 + 1\cdot 58 + 0\cdot 11 + 0\cdot 39 = 143$$

$$Y = 24 \to \underline{1}\,\underline{1}\,\underline{0}\,\underline{0}\,\underline{0} \to x_3 = 0\cdot 34 + 0\cdot 51 + 0\cdot 58 + 1\cdot 11 + 1\cdot 39 = 50$$

Decriptarea:

$$V = (34\cdot 18, 51\cdot 18, 58\cdot 18, 11\cdot 18, 39\cdot 18) \pmod{61}$$

$$V = (2, 3, 7, 15, 31)$$

$$148\cdot 18 = 41 \to (1,0,1,1,0) = 22 = W$$

$$143\cdot 18 = 12 \to (0,0,1,1,1) = 7 = H$$

$$50\cdot 18 = 46 \to (1,1,0,0,0) = 24 - Y$$