Day 06 - Merkle-Hellman Knapsack cipher

## Hill cipher

Definition 1. Hill cipher is a block cipher where pairs of plaintext letters are encrypted by the transformation

$$\begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = A \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \mod 26$$

A: 2x2 matrix that is invertible mod 2G

Remark:

. Extend the algorithm to any modulo N where N=# letters in the alphabet .

. Use any nxn invertible matrix A (under mod N)

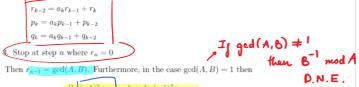
( ) To juid A - 1 mod N: use a modified Gauss - Jordan elin.

## Euclidean algorithm - Berlekamp version

The Euclidean algorithm is the process which yields the greatest common divisor d of two given integers A and B where A>B. The Berlekamp's algorithm is a slight modification of the Euclidean algorithm that can also give us the inverse of  $B \mod A$ . -> B = under mod A

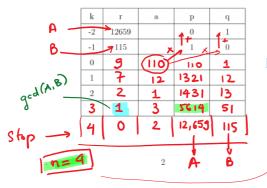
## Algorithm:

- 1. Set  $r_{-2} = A, r_{-1} = B, p_{-2} = 0, p_{-1} = 1, q_{-2} = 1, q_{-1} = 0$
- 2. For each  $k = 0, 1, 2, \dots$  compute the following



B- under mod A.

Example. Find the inverse of 115 in modulo 12659,



## Subset-Sum Problem (SSP)

Given an increasing sequence  $a_1 < a_2 < \ldots < a_n$  and a "target" number M. We want to determine if there is a subsequence of the  $a_i$ 's whose sum is t.

Formally, we want to find the values  $x_1, x_2, \dots, x_n$ , where each  $x_i$  is either 0 or 1 such that

$$x_1a_1 + x_2a_2 + \cdots + x_na_n = M.$$

**Example.** Solve the SSP for  $a_1=3, a_2=5, a_3=11, a_4=23, a_5=51,$  and M = 67.

$$67 = 51 + 16$$

$$= 51 + 11 + 5$$

$$G_7 = Q_2 + Q_3 + Q_5 = 0.a_1 + 1.a_2 + 1.a_3 + 0.a_4 + 1.a_5.$$

$$X = (0, 1, 1, 0, 1)$$

If the  $a_i$ 's form a super-increasing sequence then for every right-hand side M, the SSP either has no solution or a unique solution.

 $\begin{array}{c} \textbf{Definition 2.} \ A \ \text{super-increasing sequence} \ is \ a \ sequence \ where \ \underline{each} \ \underline{number} \\ \hline in \ \underline{the} \ \underline{sequence} \ is \ \underline{greater} \ \underline{than} \ \underline{the} \ \underline{super-increasing} \ \underline{sequence} \ if \ \underline{for \ all} \ 1 \leq k \leq n, \\ \hline Formally, \ a_1, \ a_2, \dots, \ a_n \ is \ a \ \underline{super-increasing} \ \underline{sequence} \ if \ for \ \underline{all} \ 1 \leq k \leq n, \\ \hline \end{array}$ 

$$a_k > \sum_{i=0}^{k-1} a_i$$
.

Example.

- 3>0, 5>3, 11>5+3, 23>11+5+3 51>28+11+5+3 12=7+4+11. (3,5,11,23,51)
- 2. (1, 4, 7, 12, 19)
- 3. (13, 18, 35, 72, 155, 301, 595) (You check)

**Example.** Solve the SSP for M=1003 and the super-increasing sequence

(13, 18, 35, 72, 155, 301, 595).

$$1003 = 595 + 408$$

$$= 595 + 301 + 107$$

$$= 595 + 301 + 72 + 35$$

$$= 595 + 301 + 72 + 35 + 0$$

$$1803 = 0.13 + 0.18 + 1.35 + 1.72$$

$$+ 0.155 + 1.301 + 1.595$$

$$* = (0,0,1,1,0,1,1)$$

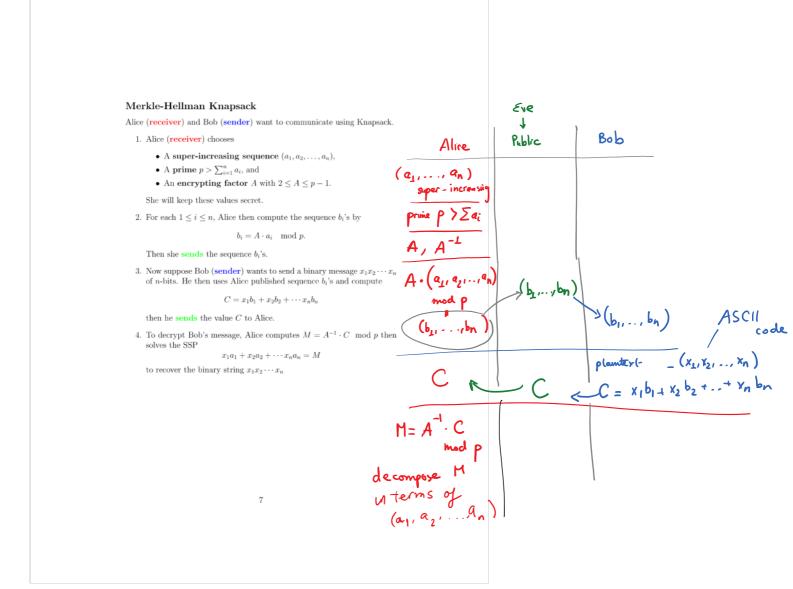
 $\begin{array}{l} \underline{\text{Remark:}} \text{ If the given sequence is not super-increasing, then the solution may not be unique.} \\ \underline{\text{Example.}} \text{ Consider } \underline{M=20} \text{ and the sequence } (1,2,3,4,5,6,7). \end{array}$ 

5

The ASCII (American Standard Code for Information Interchange) Table:

Dec	Bin	Hex	Char	Dec	Bin	Hex	Char	Dec	Bin	Hex	${\tt Char}$	Dec	Bin	Hex	Char
0	0000 0000	00	[NUL]	32	0010 0000	20	space	64	0100 0000	40	9	96	0110 0000	60	*
1	0000 0001	01	[SOH]	33	0010 0001	21	!	65	0100 0001	41	A	97	0110 0001	61	a
2	0000 0010	02	[STX]	34	0010 0010	22		66	0100 0010	42	В	98	0110 0010	62	b
3	0000 0011	03	[ETX]	35	0010 0011	23	#	67	0100 0011	43	C	99	0110 0011	63	С
4	0000 0100	04	[EOT]	36	0010 0100	24	\$	68	0100 0100	44	D	100	0110 0100	64	d
5	0000 0101	05	[ENQ]	37	0010 0101	25	8	69	0100 0101	45	E	101	0110 0101	65	e
6	0000 0110	06	[ACK]	38	0010 0110	26	£	70	0100 0110	46	F	102	0110 0110	66	£
7	0000 0111	07	[BEL]	39	0010 0111	27		71	0100 0111	47	G	103	0110 0111	67	g
8	0000 1000	80	[BS]	40	0010 1000	28	(	72	0100 1000	48	H	104	0110 1000	68	h
9	0000 1001	09	[TAB]	41	0010 1001	29	)	73	0100 1001	49	1	105	0110 1001	69	i
10	0000 1010	A0	[LF]	42	0010 1010	2A	*	74	0100 1010	4A	J	106	0110 1010	6A	j
11	0000 1011	0B	[VT]	43	0010 1011	2B	+	75	0100 1011	4B	K	107	0110 1011	6B	k
12	0000 1100	0C	[FF]	44	0010 1100	2C	,	76	0100 1100	4C	L	108	0110 1100	6C	1
13	0000 1101	0D	[CR]	45	0010 1101	2D	-	77	0100 1101	4D	м	109	0110 1101	6D	m.
14	0000 1110	0E	[SO]	46	0010 1110	2E		78	0100 1110	4E	N	110	0110 1110	6E	n
15	0000 1111	0F	[SI]	47	0010 1111	2F	/	79	0100 1111	4F	0	111	0110 1111	6F	0
16	0001 0000	10	[DLE]	48	0011 0000	30	0	80	0101 0000	50	P	112	0111 0000	70	p
17	0001 0001	11	[DC1]	49	0011 0001	31	1	81	0101 0001	51	Q	113	0111 0001	71	q
18	0001 0010	12	[DC2]	50	0011 0010	32	2	82	0101 0010	52	R	114	0111 0010	72	r
19	0001 0011	13	[DC3]	51	0011 0011	33	3	83	0101 0011	53	s	115	0111 0011	73	5
20	0001 0100	14	[DC4]	52	0011 0100	34	4	84	0101 0100	54	T	116	0111 0100	74	t
21	0001 0101	15	[NAK]	53	0011 0101	35	5	85	0101 0101	55	U	117	0111 0101	75	u
22	0001 0110	16	[SYN]	54	0011 0110	36	6	86	0101 0110	56	v	118	0111 0110	76	v
23	0001 0111	17	[ETB]	55	0011 0111	37	7	87	0101 0111	57	w	119	0111 0111	77	w
24	0001 1000	18	[CAN]	56	0011 1000	38	8	88	0101 1000	58	x	120	0111 1000	78	×
25	0001 1001	19	[EM]	57	0011 1001	39	9	89	0101 1001	59	Y	121	0111 1001	79	У
26	0001 1010	1A	[SUB]	58	0011 1010	3A	:	90	0101 1010	5A	z	122	0111 1010	7A	z
27	0001 1011	1B	[ESC]	59	0011 1011	3B	;	91	0101 1011	5B	[	123	0111 1011	7B	(
28	0001 1100	1C	[FS]	60	0011 1100	3C	<	92	0101 1100	5C	\	124	0111 1100	7C	ı
29	0001 1101	1D	[GS]	61	0011 1101	3D	-	93	0101 1101	5D	]	125	0111 1101	7D	}
30	0001 1110	1E	[RS]	62	0011 1110	3E	>	94	0101 1110	5E	^	126	0111 1110	7E	~
31	0001 1111	1F	[US]	63	0011 1111	3 <b>F</b>	?	95	0101 1111	5F	_	127	0111 1111	7 <b>F</b>	[DEL

6



 ${\bf Example.}$  Alice picks the super increasing sequence  $(a_1, a_2, \dots, a_8) = (2, 5, 9, 22, 47, 99, 203, 409)$ the prime p=997 and the encryption factor A=60. a. Compute the sequence  $b_i$ 's that Alice will publish b. Suppose Bob wants to send the letter "b" (ASCII code: 01100010) to Alice. Find his ciphertext C.c. Suppose Alice receives C=1255 from Bob. Decrypt this message.