Skapa ett chiffer

Information till läraren

Mål med problemet

Få en övergripande kunskap om hur ett chiffer fungerar och en introduktion till kryptering.

Förkunskaper

Grundläggande programmeringskunskap. If-satser, loopar.

matgymkand@gmail.com

Övergripande upplägg

Introduktion

Diskussion i helklass

- Vad är ett chiffer?
- Hur kan man kryptera ett meddelande?

Introducera elever till en ASCII-tabell (om möjlighet finns så kan den vara uppe på exempelvis en projektor under lektionen, bild finns i appendix).

Genomförande

Eleverna arbetar förslagsvis i grupper om 2 (alternativt 3 i en grupp). Här får eleverna konstruera en slags krypteringsalgoritm där inputen är en sträng innehållandes ett ord eller mening som ska krypteras, förslagsvis med hjälp av ett Caesarchiffer.

Därefter kan man gå ihop två grupper så att den andra gruppen kan skriva in en mening eller ord, så kan man sedan dekryptera det som den andra gruppen skrev.

Diskussion

I helklass

- Kunde ni tyda varandras krypteringar? Hur gjorde ni?
- Hur hade man kunnat göra för att göra det ännu svårare att dekryptera?

Ytterligare information

Bakgrund

Att vilja skicka hemliga meddelande till varandra är något som man har gjort i tusentals år. Bland den tidigaste krypterade informationen man har hittat är användandet av unika hieroglyfer i egyptiska kryptor. En flitig användare av chiffer var Julius Caesar som ofta dolde sin text genom att förskjuta bokstävernas platser i alfabetet, och därifrån har vi fått det så kallade Caesarchiffret. Den här typen av simpla chiffer såg flitig användning fram tills att datorer kunde lösa de för snabbt, och idag används mycket mer avancerade metoder för att kryptera text.

Lösningsförslag

Här löser jag problemet med Caesarchiffer, och har helt enkelt tagit ut motsvarande värde i ASCII-tabellen för sedan teckenvis addera ett visst förskjutningsvärde och göra om det till en karaktär igen, som motsvarar det nya värdet i ASCII-tabellen. I exemplet så tas inte ställning till att det krypterade tecknet ska bli en ny bokstav, då vi inte ville blanda in moduloräkning. Huruvida ni vill avgränsa problemet är givetvis upp till er.

Lösningsförslag: https://pastebin.com/F1Jc73sL

Appendix

ASCII TABLE

Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char
0	0	[NULL]	32	20	[SPACE]	64	40	@	96	60	`
1	1	[START OF HEADING]	33	21	!	65	41	A	97	61	a
2	2	[START OF TEXT]	34	22	"	66	42	B	98	62	b
3	3	[END OF TEXT]	35	23	#	67	43	C	99	63	c
4	4	[END OF TRANSMISSION]	36	24	$	68	44	D	100	64	d
5	5	[ENQUIRY]	37	25	%	69	45	E	101	65	e
6	6	[ACKNOWLEDGE]	38	26	&	70	46	F	102	66	f
7	7	[BELL]	39	27	'	71	47	G	103	67	g
8	8	[BACKSPACE]	40	28	(	72	48	H	104	68	h
9	9	[HORIZONTAL TAB]	41	29	)	73	49	I	105	69	i
10	A	[LINE FEED]	42	2A	*	74	4A	J	106	6A	j
11	B	[VERTICAL TAB]	43	2B	+	75	4B	K	107	6B	k
12	C	[FORM FEED]	44	2C	,	76	4C	L	108	6C	l
13	D	[CARRIAGE RETURN]	45	2D	-	77	4D	M	109	6D	m
14	E	[SHIFT OUT]	46	2E	.	78	4E	N	110	6E	n
15	F	[SHIFT IN]	47	2F	/	79	4F	O	111	6F	o
16	10	[DATA LINK ESCAPE]	48	30	0	80	50	P	112	70	p
17	11	[DEVICE CONTROL 1]	49	31	1	81	51	Q	113	71	q
18	12	[DEVICE CONTROL 2]	50	32	2	82	52	R	114	72	r
19	13	[DEVICE CONTROL 3]	51	33	3	83	53	S	115	73	s
20	14	[DEVICE CONTROL 4]	52	34	4	84	54	T	116	74	t
21	15	[NEGATIVE ACKNOWLEDGE]	53	35	5	85	55	U	117	75	u
22	16	[SYNCHRONOUS IDLE]	54	36	6	86	56	V	118	76	v
23	17	[ENG OF TRANS. BLOCK]	55	37	7	87	57	W	119	77	w
24	18	[CANCEL]	56	38	8	88	58	X	120	78	x
25	19	[END OF MEDIUM]	57	39	9	89	59	Y	121	79	y
26	1A	[SUBSTITUTE]	58	3A	:	90	5A	Z	122	7A	z
27	1B	[ESCAPE]	59	3B	;	91	5B	[	123	7B	{
28	1C	[FILE SEPARATOR]	60	3C	<	92	5C	\	124	7C	|
29	1D	[GROUP SEPARATOR]	61	3D	=	93	5D	]	125	7D	}
30	1E	[RECORD SEPARATOR]	62	3E	>	94	5E	^	126	7E	~
31	1F	[UNIT SEPARATOR]	63	3F	?	95	5F	_	127	7F	[DEL]

matgymkand@gmail.com