

Pienryhmätehtävät 3 - Viikolle 39

- (1) Caesar-salaus. Ohessa taulukko kirjainten “numerovastaavuuksista”

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Pura seuraavat salaukset:

- (i) NBUFNBUIJLLB (Caesar-1)
 - (ii) IBVLLNND (Caesar-3)
- (2) Vigenèren salaus (Liitteenä Vigenèren neliö.)
- (i) Salaa viesti TORSTAI avainsanalla HEI.
 - (ii) Pura viesti COZDSSFXRQDIG, kun tiedät avainsanan olevan KOODI.
- (3) (i) Olkoot $\sigma, \tau : \{1, 2, 3, 4\} \rightarrow \{1, 2, 3, 4\}$ permutaatioita ja $\sigma = (132)$ ja $\tau = (143)$. Laske permutaatioiden tulo $\sigma \circ \tau$.
- (ii) Saat englanninkielisen salaviestin (tällöin aakkosissa on 26 kirjainta). Viestin sanat on muutettu numeroiksi ja salattu eri menetelmillä. Avaa salaukset ja muuta lopuksi numerot niitä vastaaviksi kirjaimiksi (ts. $A = 1, B = 2, \dots$).
- (10 18 7) (Käytetty salausmenetelmä: Caesar)
 - (17 2 18 6 1 7) (Käytetty salausmenetelmä: ROT13)
 - (16 12 1 25) (Käytetty salausmenetelmä: identtinen kuvaus)
 - (4 5 3) (Käytetty salausmenetelmä: kertominen vasemmalta permutaatiolla (9 5 4 3), ts. $(9 5 4 3) \circ (\text{salattu sana numeroina}) = (4 5 3)$).
- (4) Tutki (pikku-)Enigman mallia ja toimintaa.
- (5) Salauksien jakoa. Suuryhtiön kassaholvin pin-koodi on jokin nelinumeroinen luku. Kolme pääjehua luottavat melkein toisiinsa. He haluaisivat kehittää menetelmän, jonka avulla holvi voidaan lukita siten, ettei kukaan saa holvia auki yksin, mutta ketkä tahansa kaksi kolmesta pääjehusta saavat sen auki yhdessä.
- Käytännössä pääjehuilla voi olla vaikka tietokone, joka joka avauksen jälkeen asettaa holviin uuden pin-koodin ja jakaa pääjehuille henkilökohtaiset koodit, joista voi mistä tahansa kahdesta päätellä varsinaisen pin-koodin. Miten tämän voi toteuttaa?
- Lisärajoite 1: Järjestelmän pitää toimia myös jos pääjehujen määrä kasvaa kymmeneen.

Lisärajoite 2: Turvallisuus. Jos joku ulkopuolinen saa käsiinsä yhden avaimen, niin koodin arvaamisen pitää olla yhtä hankalaa kuin jos hänellä ei olisi yhtään avainta.

Lisärajoite 3: Kymmenen pääjehua, joista kenen tahansa kolmen pitää saada holvi auki yhdessä. Se, että käsillä on yksi tai kaksi avainta, ei saa tehdä holvin luvatta avaamisesta helpompaa, kuin jos käsillä olisi vain yksi avain.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Kuva 1: Vigenèren neliö Vigenère-salauksen avuksi