Šifravimo ir kibernetinio saugumo užduotys

Kokias užduotis galima duoti 5-8 kl. mokiniams

Simona Ramanauskaitė

Ką ir kaip mokyti pagal atnaujintą programą?

Nurodymai rekomendacinio pobūdžio

Mokytojui paliekama laisvė rinktis būdus ir turinį

Papildomos idėjos 5-8 klasių mokytojams

Numatytos saugos temos ir jų įsisavinimui galimi spręsti uždaviniai

Klasė	Tema	Aprašymas	Užduočių idėjos	Užduočių pavyzdžiai
5-6	6.3.3.7. Duomenų ir informacijos privatumo, saugumo problemos.	Mokytojas aptaria su mokiniais duomenų privatumo ir saugumo problemas, pateikia ir nagrinėja konkrečius pavyzdžius. Mokiniai mokomi tyrinėti surinktus duomenis, įvertinti, ar jie tinka duotam uždaviniui spręsti.	Pateikiami pavyzdžiai kada sistema, mobili programa prašo tam tikrų duomenų ar teisių. Klausiama kam tokių duomenų galėtų reikėti, ar jie nėra pertekliniai.	Nueikite į Google Play programą ir pasirinkite atitinkamą mobilią programą (pvz. Instagram). Prie aprašymo peržiūrėkite duomenų saugos bloką. Prie kiekvieno punkto apie bendrinamus arba surinktus duomenis parašykite: kam tie duomenys gali būti naudojami toje programoje, kokia jų paskirtis; ar tie duomenys nėra pertekliniai, gali jums pakenkti arba per daug atskleisti informacijos apie jus.
				Nueikite į Telefono nustatymus, pasirinkite skiltį Programos. Pasirinkite vieną iš programų (pvz. facebook). Pasirinkite programų leidimai skiltį. Prie kiekvieno leidimo nurodykite: kam šiai programai gali būti reikalingas šis leidimas; kaip šis leidimas gali būti panaudojamas prieš jus (gauti jūsų nenorimų dalinti duomenų ar juos rinkti jums nežinant); kokias teises siūlytumėte šiai prieigai, kad būtumėte saugūs ir apsaugotumėte savo privatumą (leidžiama visada, klausti kaskart, neleidžiama visai).
		Toliau gilinamasi į duomenų ir informacijos patikimumo problemą. Mokiniai skatinami įsitikinti, ar surinkti duomenys ar rasta	Rodyti įvairius duomenų šaltinius ir klausti ar juose pateikiama informacija,	Nueiti į naujienų portalą, kur rašomi komentarai. Pasirinkti vieną iš komentarų ir klausti: ar komentare rašoma teisybė? Kas parašė tą komentarą? Ką mes dar žinome apie to

http://mima112.eu/vt/Saugos_uzdaviniai_mokiniams.pdf

Keletas labiau interaktyvių pavyzdžių

5-6 kl. – 6.3.3.8. Šifravimo uždaviniai

- Retai naudojamos kalbos naudojimas apsunkina aplinkiniams suvokimą apie ką kiti asmenys kalba
- Susikurti savo kalbą gali būti sunku, bet galima pakoreguoti kalbą, kad ji būtų ne taip lengvai perprantama aplinkiniams

- Pasakykite po sakinį apie save, prieš kiekvieną skiemenį pasakydami savo vardo pirmą skiemenį ar kitą pasirinktą skiemenį.
  - Pavyzdžiui: Sisveisiki, simasino sivarsidas sisisimosina.

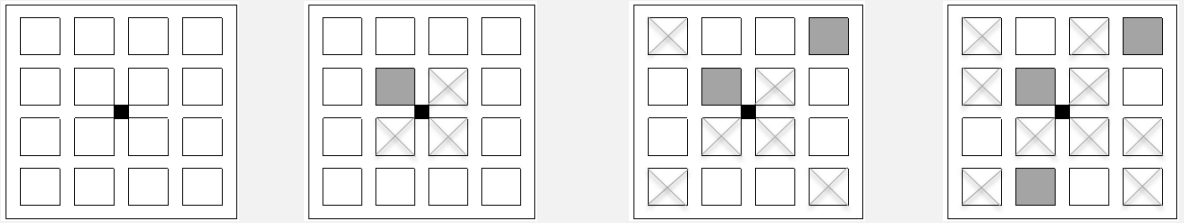
5-6 kl. – 6.3.3.8. Šifravimo uždaviniai

- Siųstas pranešimas
  - „PRESIDENT'S EMBARGO RULING SHOULD HAVE IMMEDIATE NOTICE. GRAVE SITUATION AFFECTING INTERNATIONAL LAW. STATEMENT FORESHADOWS RUIN OF MANY NEUTRALS. YELLOW JOURNALS UNIFYING NATIONAL EXCITEMENT IMMENSELY“.
- Tikroji žinutė buvo „Pershing sails from N.Y. June I“

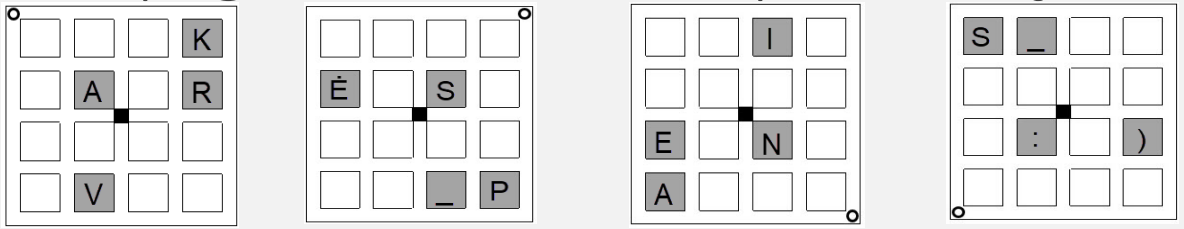
- Kaip buvo perskaityta tikroji žinutė?
- Parašykite pranešimą, kuriame būtų paslėpta žinutė, atitinkanti jūsų vardą. Pavyzdžiui:
  - Spintelėje ilgai mėtėsi obuolys, noko ananasas.

5-6 kl. – 6.3.3.8. Šifravimo uždaviniai
7-8 kl. – 6.4.3.4. Šifravimo metodai, simetrinio rakto kriptografinė sistema

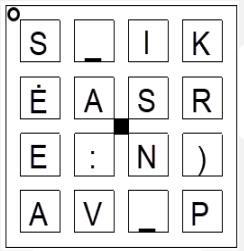
- Šifravimo raktas gali būti ne tik duomenys, bet ir objektas
- Pasidarykite savo šabloną duomenų kodavimui



- Jo pagalba užšifruokite pasirinktą žinutę

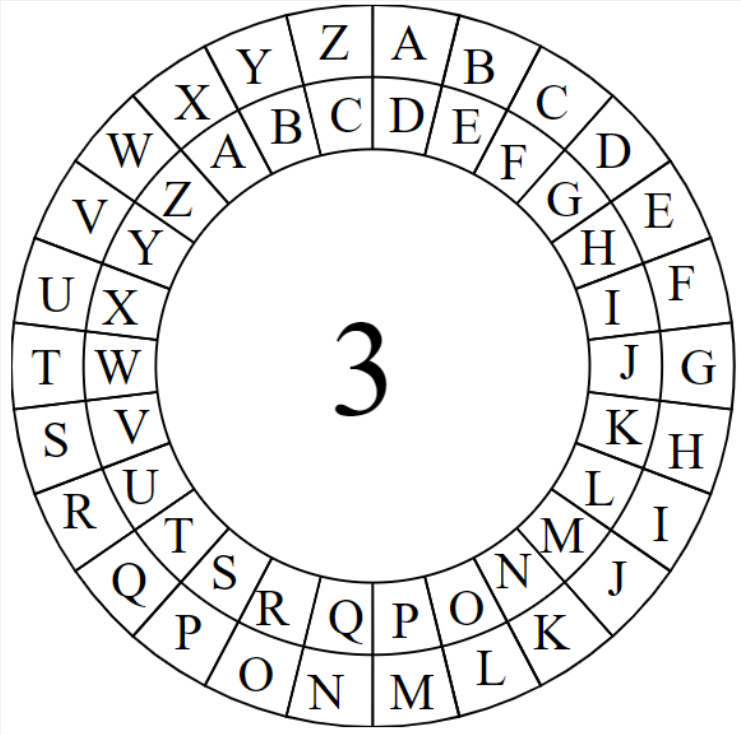


- Atšifruokite žinutę ar raskite gautam šifrui tinkamą raktą



5-6 kl. – 6.3.3.8. Šifravimo uždaviniai
7-8 kl. – 6.4.3.4. Šifravimo metodai, simetrinio rakto kriptografinė sistema

- Cezario šifravime visa abėcėlė yra paslenkama per raktą
- Raktas yra skaičius, nusakantis kiek pastumti abėcėlę
  - Pavyzdyje raktas yra 3, todėl vietoj raidės A tekste rašysime D, vietoj B – E, C – F, ...
- Šifruojant raidę keičiame į paslinktą dešiniau per rakto dydį
- Dešifruojant raides kečiame pereinant kairėn abėcėle per rakto dydį
- Paprastumo dėlei galima susidaryti savo abėcėlės pastūmimo atitikmenį

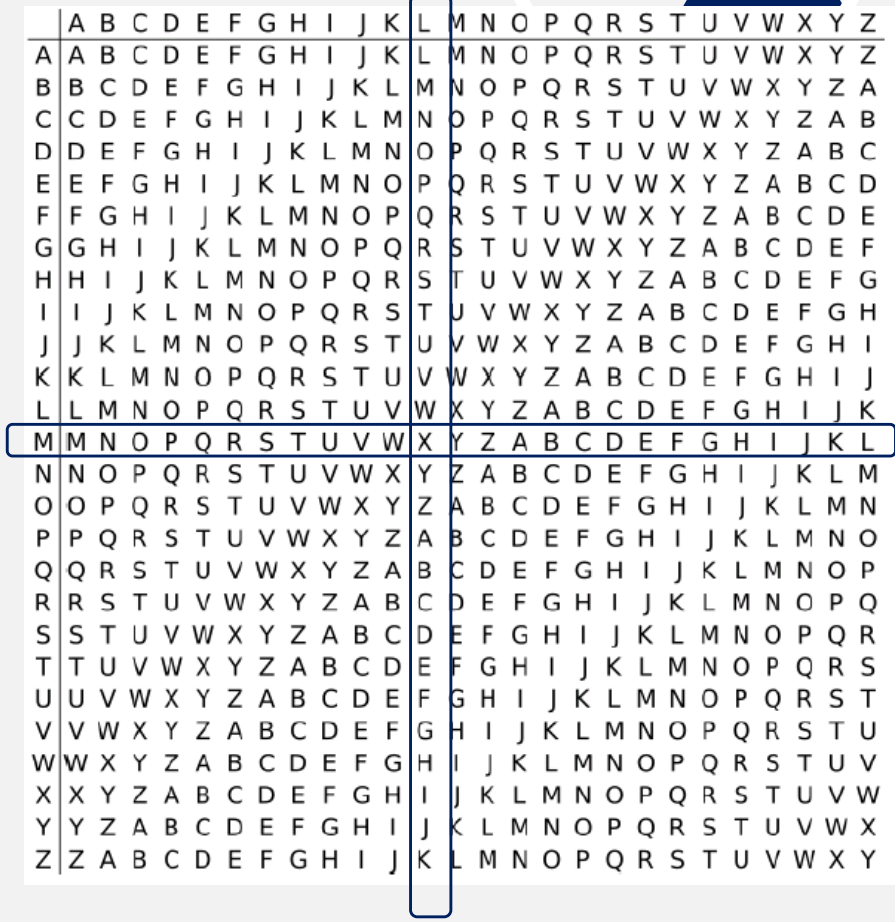


5-6 kl. – 6.3.3.8. Šifravimo uždaviniai
7-8 kl. – 6.4.3.4. Šifravimo metodai, simetrinio rakto kriptografinė sistema

- Turima lotyniška abėcėlė ABCDEFGHIJKLMNOPQRSTUVWXYZ
  Naudojamas šifravimo raktas 5. Reikia užšifruoti frazę RAUDONA ZONA
  - Koks bus gautas kodas?
- Turima lotyniška abėcėlė ABCDEFGHIJKLMNOPQRSTUVWXYZ
  Naudojamas šifravimo raktas 3. Reikia atšifruoti šifrą EDOWDV ODQJV
  - Koks bus gautas tekstas?
- Turima lotyniška abėcėlė ABCDEFGHIJKLMNOPQRSTUVWXYZ
  Nežinomas šifravimo raktas. Reikia atšifruoti šifrą QTCU
  - Koks galėtų būti gautas tekstas?

7-8 kl. – 6.4.3.4. Šifravimo metodai, simetrinio rakto kriptografinė sistema

- Pasimatė, kad Caesar šifravimas nėra saugus, tad kaip galima pasunkinti šį kodą?
  - Mūsų raktas gali būti taip pat tekstas
  - Kiekvienas teksto simbolis koduojamas su atitinkamu rakto simboliu – jų susikirtime gaunamas šifras
  - Jei raktas trumpesnis nei tekstas – raktas kartojamas
  - Dešifruojant rakto eilutėje/stulpelyje ieškoma kodo simbolio ir taip stulpelyje/eilutėje matomas tikrasis simbolis
    - Tekstas: LABAS
    - Raktas MES
    - Kodas: XETMW
- Užšifruokite savo pavardę, kaip raktą naudodami vardą



	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

7-8 kl. – 6.4.3.4. Šifravimo metodai, simetrinio rakto kriptografinė sistema

- Patikrinkite ar teisingai užkodavote savo pavardę tinklalapyje https://www.dcode.fr/vigenere-cipher
- Ten pat patikrinkite ar gausite tokį patį kodą, jei naudosite lietuvišką abėcėlę

7-8 kl. – 6.4.5.6. Slaptažodis

- Apsilankykite svetainėje https://www.passwordmonster.com/
- Įvertinkite kiek laiko reikėtų norint atspėti šiuos slaptažodžius:
  - admin123456
  - 123house456
  - 123namas456
  - <_n4m4s_>
  - _jwkwe_
- Kas sugalvosite „ilgiausiai laužiamą“ slaptažodį, kuris reikštų „kaktusas“, būtų lengvai atsimenamas, bet kuo sudėtingesnis atspėti
  - Išrinksime ilgiausiai nulaužiamą tarp tų, kurie tikrai reikš kaktusą

7-8 kl. – 6.4.5.5. Informacijos apie save pateikimas internete

Užsiregistruokite svetainėje
http://mima112.eu/login
bet **nenaudokite** savo **įprastų prisijungimų**

Tokio sudėtingumo slaptažodžius naudoja mokiniai

VILNIUS TECH

Nr.	Vartotojas	Slaptažodis		
		Dalinai paslėptas	Statistika	MD5 reikšmė
1	admin	****n	0 skaičių, 5 mažųjų lotyniškų raidžių, 0 didžiųjų lotyniškų raidžių, 0 kitų simbolių.	21232f297a57a5a743894a0e4a801fc3
2	admin	****n	0 skaičių, 5 mažųjų lotyniškų raidžių, 0 didžiųjų lotyniškų raidžių, 0 kitų simbolių.	21232f297a57a5a743894a0e4a801fc3
3	admin	****3***	4 skaičių, 0 mažųjų lotyniškų raidžių, 0 didžiųjų lotyniškų raidžių, 0 kitų simbolių.	d54d1702ad0f8326224b817c796763c9
4	admin	****m****n	0 skaičių, 5 mažųjų lotyniškų raidžių, 0 didžiųjų lotyniškų raidžių, 0 kitų simbolių.	accb67dabfb709dd58931f5ffd4f0032
5	alphapatinas	****s****s	0 skaičių, 4 mažųjų lotyniškų raidžių, 0 didžiųjų lotyniškų raidžių, 0 kitų simbolių.	07f043935f9198f29c102e457f37e2a7
6	ameba	****a****i****s	0 skaičių, 10 mažųjų lotyniškų raidžių, 0 didžiųjų lotyniškų raidžių, 0 kitų simbolių.	9726ee5b301a7da4898e28e5b108b867
7	briaunainis	****u****k****0****0**	5 skaičių, 11 mažųjų lotyniškų raidžių, 0 didžiųjų lotyniškų raidžių, 1 kitų simbolių.	420f651dad295ab1a558097dc99401e6
8	Emuteaa	****k****s	0 skaičių, 7 mažųjų lotyniškų raidžių, 1 didžiųjų lotyniškų raidžių, 2 kitų simbolių.	e4b3e9bb3aaf7e0594a4eb455d01b451
9	europa	****r****k****9*	4 skaičių, 7 mažųjų lotyniškų raidžių, 0 didžiųjų lotyniškų raidžių, 0 kitų simbolių.	bafaf3c7f43f7162fbedf161015ed28b
10	Hisenburg	****	0 skaičių, 4 mažųjų lotyniškų raidžių, 0 didžiųjų lotyniškų raidžių, 0 kitų simbolių.	fed1f37d40a3e8a0103bf5e95875a82f
11	jonas	****u****2*	3 skaičių, 6 mažųjų lotyniškų raidžių, 0 didžiųjų lotyniškų raidžių, 0 kitų simbolių.	baf50bfab189c95c00d544238b097cf1
12	jonas	****s	0 skaičių, 5 mažųjų lotyniškų raidžių, 0 didžiųjų lotyniškų raidžių, 0 kitų simbolių.	9c5ddd54107734f7d18335a5245c286b
13	labas123	****s****	4 skaičių, 3 mažųjų lotyniškų raidžių, 1 didžiųjų lotyniškų raidžių, 0 kitų simbolių.	cd6bd07b905063267be8cf21885820de
14	lalala	****m***	0 skaičių, 2 mažųjų lotyniškų raidžių, 0 didžiųjų lotyniškų raidžių, 0 kitų simbolių.	877dba90e1752571ffa32de87602981e
15	LBenas	****s*	0 skaičių, 4 mažųjų lotyniškų raidžių, 1 didžiųjų lotyniškų raidžių, 0 kitų simbolių.	d1bb669448e021c8a7875577e674c083
16	neidazy	****t****a****	0 skaičių, 10 mažųjų lotyniškų raidžių, 0 didžiųjų lotyniškų raidžių, 0 kitų simbolių.	712bf69150b997bfa53d2df53195bd40
17	pelke	****a****v****m	0 skaičių, 10 mažųjų lotyniškų raidžių, 2 didžiųjų lotyniškų raidžių, 0 kitų simbolių.	aa6662e2d1c043fa9d62cc4b1a092b23
18	Petras	****a****s**	2 skaičių, 8 mažųjų lotyniškų raidžių, 0 didžiųjų lotyniškų raidžių, 0 kitų simbolių.	6c89d29808bf53f48b2c2de6eb23a384
19	poopfart	****k****2*	3 skaičių, 8 mažųjų lotyniškų raidžių, 0 didžiųjų lotyniškų raidžių, 0 kitų simbolių.	5c7a4b7327aa3daaa07be9b4b6b1aa2f
20	prdou	****n****r**	4 skaičių, 6 mažųjų lotyniškų raidžių, 0 didžiųjų lotyniškų raidžių, 0 kitų simbolių.	aab9e98ca38944d13e1a83944f34cb2d

5-6 kl. – 6.3.3.7. Duomenų ir informacijos privatumo, saugumo problemos

- Nueikite į Google Play programą ir pasirinkite atitinkamą mobilią programą (pvz. Instagram).
  - Prie aprašymo peržiūrėkite duomenų saugos bloką.
  - Prie kiekvieno punkto apie bendrinamus arba surinktus duomenis parašykite:
    - kam tie duomenys gali būti naudojami toje programoje, kokia jų paskirtis;
    - ar tie duomenys nėra pertekliniai, gali jums pakenkti arba per daug atskleisti informacijos apie jus.
- Nueikite į Telefono nustatymus, pasirinkite skiltį Programos. Pasirinkite vieną iš programų (pvz. facebook).
  - Pasirinkite programų leidimai skiltį.
  - Prie kiekvieno leidimo nurodykite:
    - kam šiai programai gali būti reikalingas šis leidimas;
    - kaip šis leidimas gali būti panaudojamas prieš jus (gauti jūsų nenorimų dalinti duomenų ar juos rinkti jums nežinant);
    - kokias teises siūlytumėte šiai prieigai, kad būtumėte saugūs ir apsaugotumėte savo privatumą (leidžiama visada, klausti kaskart, neleidžiama visai).

VILNIUS TECH

Ačiū už Jūsų darbą

S. Ramanauskaitė
simona.ramanauskaite@vilniustech.lt
VILNIUS TECH

MERIT