

KRIPTOLOGIJA

Simetrično šifriranje

Danas sve više ljudi uči i radi na daljinu.

Budući da radimo putem interneta, veoma je važno da zaštitimo svoje podatke.

Navedi vrste podataka koje bi htio/htjela zaštititi na internetu.

No kako da to učinimo?

Započnimo s porukom:


J B N B L J E 4 U F D I

Možeš li je pročitati? Zašto ne?

Ako si odgovorio/odgovorila zato jer je **kodirana** ili **šifrirana**, u pravu si!

Profesionalci koji izrađuju ovakve šifre pomoću matematike nazivaju se **kriptolozi**.

Tvrtka Mastercard upotrebljava **ključeve** za šifriranje informacija koje putuju njenom mrežom.

Zamisliti da imaš lokot.  Potreban ti je specifičan **ključ** da bi ga zaključao/zaključala i otključao/otkjučala.

Ukoliko isti **ključ** poruku i zaključava i otključava, to nazivamo **simetričnim šifriranjem**.

Šifriranje pretvaranje informacija u kod, posebice s ciljem sprječavanja neovlaštenog pristupa

Simetrično jednaki dijelovi okrenuti jedni prema drugima



KRIPTOLOGIJA

Simetrično šifriranje

Jedan primjer simetričnog šifriranja je **kod ROT1**.

Svako slovo se pomiče za jedan položaj.

A postaje B. B postaje C.

Kod ROT1 je **ključ** pomoću kojeg je kodirana ova poruka.

J BN B LJE 4 UFDI

Možeš li je sad pročitati? Što piše?

Pokušaj kodirati vlastitu poruku upotrebom koda ROT1.

Provjeri hoće li je drugi moći razumjeti.

Možda ćeš im morati otkriti ključ!

No što ako netko pronade, odgonetne i ukrade tvoj ključ?

Budući da isti ključ šifrira i dešifrira informacije, prilično ga je lako dekodirati.

ROT 1 KOD

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

KRIPTOLOGIJA

Tokenizacija

Što bi bilo ako bi odnos između podataka i načina na koji su šifrirani bio slučajan?

Što bi bilo ako ne bi postojao predvidljivi uzorak?

Pogledajmo još jednu poruku. Možeš li je pročitati?



Piše T O K E N I Z A C I J A

Ovo je drugi oblik šifriranja koji može zaštititi tvoje podatke.

U gore navedenim primjerima svako je slovo zamijenjeno tokenom, poput emotikona.

Koje druge vrste nasumičnih tokena ti padaju napamet?

Šifriraj svoju poruku kreiranjem vlastitih **tokena**.

Upotrijebi maštu kako bi kreirao/kreirala svoje tokene u dolje navedenoj tablici.

Tokeni mogu biti simboli, slike ili čak boje!

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

Šifrirajte svoju poruku ovdje.

Pitaj druge mogu li dekodirati tvoju tajnu poruku.

Dakle, ako razmotrimo **simetrično šifriranje** u odnosu na **tokenizaciju**, što se čini sigurnijim?

Zamisli vrata s bravom. Je li sigurnije imati jedan ključ za ulazak i izlazak? Ili veći broj ključeva i brava?

Ako si odabrao/odabrala **tokenizaciju** kao sigurniju opciju, u pravu si.

Ti si Kids4Tech kriptolog/kriptologinja!

Tokenizacija
proces zamjene
osjetljivih
podataka
neosjetljivim
„tokenom“

CERTIFIKAT O POSTIGNUČU

Čestitke!

TI SI CERTIFICIRANI/CERTIFICIRANA



ŠAMPION / ŠAMPIONKA

Michael Miebach
CEO, Mastercard

Susan Warner
Founder, Kids4Tech