SCENARIJ POUČAVANJA

Naziv scenarija	Uvod u supstitucijske šifre
Nastavni predmet i razred	Informatika, 3. razred prirodoslovno-matematičke gimnazije
Ishodi učenja	**Srednja škola** **B. 1. 1.** (pri čemu su ulazne i izlazne vrijednosti input otvorenog teksta i ključa, dok je output šifrirani tekst, glede koraka razumije kako dolazi do pomaka slova) **B. 2. 4.** (primjenjivo na posljednji ishod sata, timski dolazi do programskog rješenja Playfairove šifre) **B. 3. 6.** (usko povezano sa ostatkom gradiva i temeljima kriptografije) **Osnovna škola** **B. 5. 1.** (pri čemu su ulazne i izlazne vrijednosti input otvorenog teksta i ključa, dok je output šifrirani tekst) **B. 8. 1.** (bez prethodno viđenog koda, samostalno, na temelju teorijskih činjenica i prethodnog programerskog znanja napraviti kod koji kriptira i dekriptira unos korisnika)
Cilj, zadaci i kratki opis aktivnosti	**Cilj:** omogućiti učeničko razumijevanje ručnog razbijanja šifri (Cezarova i Viegenerova), primijeniti razumijevanje šifriranja u Python kodu, razvijanje logike kriptiranja i skrivanja podataka **Zadaci:** učenici moraju, nakon odslušanog sata, samostalno proći kroz kod i pitati eventualne nejasnoće, a za idući sat pokušati shvatiti kako funkcionira Playfairova šifra. Od ovog sata se očekuje shvaćanje jednostavnijih šifri pri čemu im se daju 2 praktična primjera da ručno kriptiraju otvoreni tekst.

SCENARIJ POUČAVANJA

	Kratki opis aktivnosti: na kraju svake cjeline objašnjenog gradiva, potiče se aktivno sudjelovanje učenika gdje moraju riješiti 2 mozgalice („Što je Cezar/Viegenere htio reći) i jedno ručno šifriranje kako bi shvatili princip ručne ciklične zamjene.
Ključni pojmovi	Kriptografija, supstitucijske šifre, enkripcija, dekripcija, Python, Cezarova šifra, Viegenereova šifra
Korelacija	Međupredmetni kurikulum (*Uporaba informacijske i komunikacijske tehnologije za osnovne i srednje škole u Republici Hrvatskoj*) ikt D.2.2. i D.3.2. sa D.4.2. i D.5.2. (npr. predlaže bolji, efikasniji kod) ikt D.2.3. i D.3.3. sa D.4.3. i D.5.3. (npr. samostalno ili timski stvara kod za iduću lekciju)
Strategije, metode i oblici učenja i poučavanja	**Strategije:** postavljanje okvira koji će u učenicima pobuditi prethodni interes (na satu prije ovoga dati *hint* što ćemo učiti i spomenuti učenicima da pročitaju kraći izvod povijesti kriptografije, tj. evolucije šifri **Metode:** suradničko učenje > učenici međusobno mogu prodiskutirati kod, pokušati „razbiti“ šifre ručno/na papiru ili predložiti bolja idejna rješenja **Oblici učenja i poučavanja** • obrnuta učionica > video predavanje im je dostupno kroz Merlin, a učenici moraju osmisliti kod koji će objediniti teorijski izneseno znanje • igrifikacija > učenici koriste igre dostupne na mrežnoj stranici CryptoClub pa na temelju otvorenog teksta prvo pokušavaju shvatiti kako šifre funkcioniraju • inkluzivan pristup > materijali dostupni svim učenicima u obliku koji odgovara personaliziranim potrebama • povezivanje sa svakodnevnim životom > povijesni razvoj kriptografije i utjecaj na današnju zaštitu podataka

SCENARIJ POUČAVANJA

	• upotreba IKT-a > korištenje interaktivnih alata poput ReplIT-a gdje učenici pokretanjem koda odmah dobivaju rješenja
Potrebni alati	Moodle, računalo s pristupom internetu, papir i olovka (za ručno razbijanje šifri ukoliko učenik ne koristi digitalni alat s kojim se može jednako dobro snaći, npr. Paint / Excel)
Materijali za nastavnike	Udžbenik, dodatna literatura u slučaju upita koji su van okvira redovnog sata („Za one koji žele znati više“)
Materijali za učenike	Literatura na stranom jeziku za naprednije učenike
Razrada aktivnosti	**Motivacijski dio** – objašnjavamo važnost supstitucijskih šifri u povijesnom kontekstu, navodimo primjere (Cezarova i Viegenereova) **Provedba aktivnosti** – prikaz postupka provođenja svake od šifri uključujući ručno (de)kriptiranje, implementacija u kodu **Evaluacijski dio** – samostalne vježbe u hodu kojima se ispituje jasnoća utvrđenog gradiva (nekad odmah nakon definicije, nekad na kraju sata), provedba povremenih pop-up pitalica sa pitanjima koja imaju ponuđene odgovore ili iziskuju izbor točno/netočno
Postupci potpore	Video je maksimalno prilagođen svim učenicima pa tako i one koji se u potpunosti oslanjaju na korištenje samo tipkovnice/miša. (Minimalno pop-upsa) Transkripcija videa dostupna je za gluhe studente, dok ne postoji audio zapis koji bi koristio slijepim/slabovidnim osobama. Kontrast pozadine i teksta je postavljen u skladu sa standardima digitalne izrade web sadržaja (izuzev žutog teksta pisanog ručno koji se vidio prije exporta). Taj dio je nadoknađen opisivanjem kroz titlove/captions. Za njih je predviđen .SRT file koji se može pretvoriti u VTT i prilagoditi za text-to-speech čitače.

SCENARIJ POUČAVANJA

	Ostale kognitivne ili fizičke poteškoće su izuzete iz ovog primjera.
Prilozi	Osim Python kodova koji su dostupni kroz ReplIT linkove (vidljivi u videu) nemam dodatnih priloga.
Korišteni izvori	Udžbenik za 3. razred prirodoslovno-matematičke gimnazije (SysPrint) i osobni materijali s Fakulteta informatike u Puli (kolegij „Kriptografija“, ak.god. 2023./2024.)

Prilozi: N/A