SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

PROJEKTNI RAD

PRIMJENA METODA KLASIČNE KRIPTOGRAFIJE NA PRIMJERU EDUKATIVNE IGRE

Dominik Arih, Emilia Haramina, Mateo Paladin,
Jakov Halić, Kristina Paleka

Zagreb, lipanj 2022.

Ovaj rad izrađen je na Fakultetu Elektrotehnike i Računarstva pod vodstvom prof. dr. sc. Lee Skorin-Kapov i predan je na natječaj za dodjelu Rektorove nagrade u akademskoj godini 2021./2022.

SADRŽAJ

1. Uvod

Potreba za sigurnom razmjenom informacija je razvojem novih oblika komunikacije postala sva prisutnija što je rezultiralo razvojem brojnih načina šifriranja, a samim time i razvojem **kriptografije** kao znanstvene discipline. Danas, u vrijeme globalnih komunikacijskih mreža, kriptografija ulazi u sve širu uporabu kako bi se uz pomoć računala mogli zaštititi podaci u digitalnom obliku. U ranijim fazama klasične kriptografije, pojavljuju se neke šifre koje se djelomično mogu smatrati pretečom modernog načina šifriranja. S obzirom na njihovu jednostavnost, takve su šifre pogodne za objašnjavanje osnovnih koncepata kriptografije.

U ovom će radu biti objašnjene osnove klasične kriptografije pri čemu se posebna pozornost pridaje simetričnom i asimetričnom načinu šifriranja. Također, opisani su dizajn i implementacija dvodimenzionalne računalne pokazne videoigre koja načine šifriranja klasične kriptografije koristi u edukativne svrhe.

Igra se temelji na igračevoj sposobnosti dešifriranja poruka, odnosno rješavanja zagonetki, pomoću ponuđenih alata i dodatnih objašnjenja. Cilj razvoja takve pokazne igre je na interaktivan način približiti spomenute koncepte igraču te podići njegovu svijest i interes za opći problem zaštite od narušavanja sigurnosti.

2. Uvod u kriptografiju

Kriptografija je znanstvena disciplina koja se bavi proučavanjem metoda za slanje poruka u takvom obliku da ih samo onaj kome su namijenjene može pročitati. Sama riječ kriptografija grčkog je porijekla i mogla bi se doslovno prevesti kao "tajnopis" [1]. Metode i tehnike kriptoanalize drastično su se mijenjale kroz povijest, prilagođavajući se rastućoj kriptografskoj složenosti, od metoda olovke i papira iz prošlosti do matematički naprednih kriptografskih rješenja današnjice.

Prije modernog doba, kriptografija je bila sinonim za enkripciju, tj. proces pretvaranja čitljivog teksta u šifrirani i nerazumljiv tekst. Tehniku dekodiranja šifriranog teksta pošiljatelj dijeli samo ciljanim primateljima i tako sprječava treću stranu da čita privatne poruke. Od razvoja rotorskih strojeva za šifriranje u Prvom svjetskom ratu i pojave računala u Drugom svjetskom ratu, metode kriptografije postale su sve složenije, a njihove primjene raznovrsnije. Cilj moderne kriptografije više nije samo povjerljivost informacija već i **integritet** poruka, **autentifikacija** pošiljatelja i primatelja te osigurana **neporecivost**.

Kriptoanaliza je disciplina dešifriranja i analiza kodova, šifri i šifriranog teksta pomoću matematičkih formula, kako bi se razumjeli skriveni aspekti sustava. Koristi se za traženje ranjivosti algoritama i provale u sigurnosne sustave iskorištavajući slabosti u implementaciji kriptografskih algoritama čak i kada je kriptografski ključ nepoznat [2][3].

2.1. Klasična kriptografija

Osnovne šifre klasične kriptografije su **transpozicijske šifre**, koje preuređuju redoslijed slova u poruci, te **supstitucijske šifre**, koje sustavno zamjenjuju slova ili grupe slova s nekim drugim grupama. Jedna od ranijih poznatih supstitucijskih šifri je **Cezarova šifra** gdje se svako slovo u tekstu mijenja slovom koje se za određeni broj slova nalazi niže u abecedi, a za zapisivanje svih povjerljivih informacija koristio ju je i sam Julije Cezar [4] [5].

Posebna vrsta kriptografije iz Antičkog doba je **steganografija**. Kako bi poruka ostala povjerljiva skrivalo se čak i njeno postojanje. Moderniji primjeri steganografije uključuju korištenje nevidljive tinte i digitalnih vodenih žigova. Za pomoć pri šifriranju korišteni su različiti uređaji, a jedan od ranijih takvih uređaja je ***scytale***. To je alat koji se koristi za izvođenje transpozicijske šifre, a sastoji se od cilindra s namotanom trakom pergamenta na kojoj je ispisana poruka. Spartanci su koristili ovu šifru za komunikaciju tijekom vojnih kampanja tako što bi primatelj koristio cilindar istog promjera na kojeg bi omotao pergament kako bi pročitao poruku.

Šifrirani tekstovi proizvedeni klasičnim metodama šifriranja u današnje vrijeme nisu pouzdani jer otkrivaju statističke podatke o otvorenom tekstu, a takve se informacije često mogu koristiti za razbijanje šifre. Nakon otkrića **frekvencijske analize** takve metode šifriranja i dalje su popularnost, no uglavnom samo kao zagonetke. Korištenjem različitih šifri za različite dijelove poruke nastale su **polialfabetske šifre** koje su otpornije na frekvencijsku analizu. Primjer takve šifre je **Vigenèreova šifra** gdje enkripcija koristi ključnu riječ koja kontrolira zamjenu slova ovisno o tome koje se slovo ključne riječi koristi.

U 19. stoljeću konačno je prepoznato da tajnost algoritma šifre nije razumna niti praktična zaštita sigurnosti poruka te da svaka adekvatna kriptografska shema treba ostati sigurna čak i ako protivnik u potpunosti razumije sam algoritam šifriranja. Sigurnost korištenog ključa trebala bi biti dovoljna da dobra šifra zadrži povjerljivost u slučaju napada [6]. Ovo načelo naziva se **Kerckhoffsov princip** (eng. *Kerckhoffs's principle*). Općenitije načelo je **savršena povjerljivost** koje govori kako šifra pruža povjerljivost ako je za svakog napadača šansa da pogodi poruku jednaka [7].

2.2. Moderna kriptografija

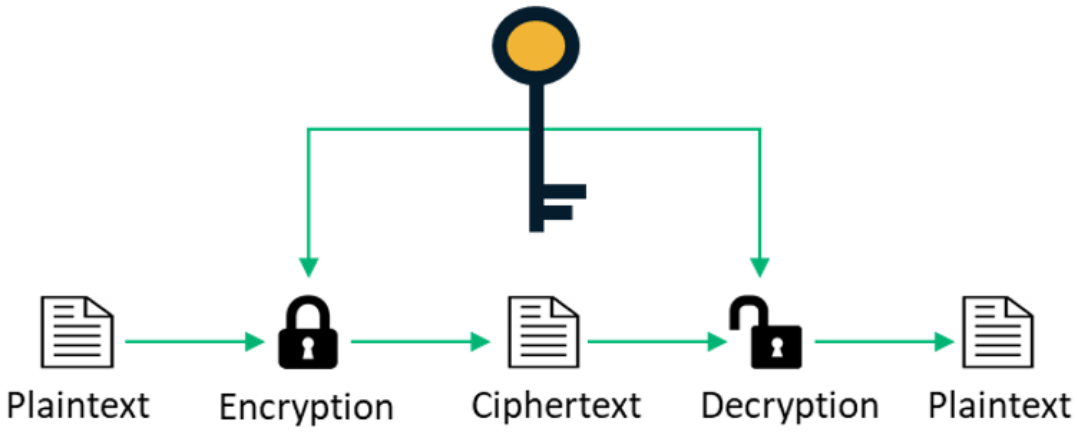
Od razvoja rotorskih strojeva za šifriranje u Prvom svjetskom ratu i pojave računala u Drugom svjetskom ratu, metode kriptografije postale su sve složenije, a njihove primjene raznovrsnije. Prije početka 20. stoljeća, kriptografija se uglavnom bavila lingvističkim i leksikografskim obrascima [4]. Moderna kriptografija uvelike se temelji na matematičkoj teoriji uključujući aspekte teorije informacija, računske složenosti, statistike, kombinatorike, apstraktne algebre i teorije brojeva. Razvoj digitalnih računala i elektronike omogućio je mnogo složenije šifre te računala dopuštaju šifriranje bilo koje vrste podataka u binarnom formatu, za razliku od klasičnih šifri koje su šifrirale samo pisane tekstove. Računalne šifre rade s binarnim nizovima bitova, a klasične općenito izravno manipuliraju slovima i znamenkama te je tako upotreba računala is-

tisnula lingvističku kriptografiju.

Početkom 1970-ih dizajniran je algoritam za šifriranje podataka (**DES**) koji je postao prvi kriptografski standard savezne vlade u Sjedinjenim Državama. Algoritam je zasnovan na **Feistelovoj šifri**. Feistelova struktura implementira niz iterativnih šifri za blok podataka i općenito je dizajnirana za blok šifre koje šifriraju velike količine podataka [8]. Gotovo svi simetrični blokovni algoritmi koji su danas u uporabi koriste spomenuti algoritam [1]. Jedna od glavnih ideja je alternirana uporaba supstitucija i transpozicija kroz više iteracija (tzv. rundi).

2.2.1. Simetrična kriptografija

Kriptografija simetričnim ključem odnosi se na metode šifriranja u kojima i pošiljatelj i primatelj dijele isti ključ. Slika 2.1 prikazuje princip šifriranja čistog teksta nekim ključem pri čemu se dobiva šifrat. Iz šifrata postupkom dekripcije tim istim ključem ponovno nastaje čisti tekst.



Slika 2.1: Princip rada simetrične šifre, slika preuzeta iz [9]

Standard enkripcije podataka (**DES**) i napredni standard enkripcije podataka (**AES**) su primjeri **blok šifriranja** koje je američka vlada odredila kao standarde kriptografije [4]. Unatoč tome što je odbačen kao službeni standard, DES i 3DES varijanta koriste se i dalje u širokom rasponu aplikacija. Osmišljene su i objavljene mnoge druge blok šifre, sa značajnim varijacijama u kvaliteti, poput **IDEA** i **Blowfish**.

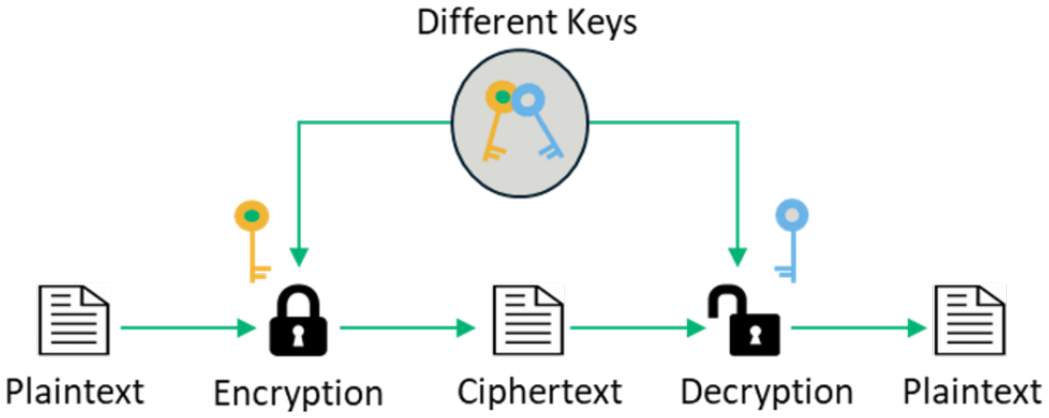
Protočne šifre, za razliku od blok šifri stvaraju proizvoljno dug tok ključnog materijala, koji je kombiniran s otvorenim tekstom bit-po-bit ili znak-po-znak [7]. U protočnoj šifri, izlazni tok se kreira na temelju skrivenog unutarnjeg stanja koje se mijenja kako šifra radi. To interno stanje u početku se postavlja pomoću materijala tajnog

ključa. **RC4** je široko korištena protočna šifra, a postoje i **CSS** te **Salsa20/ChaCha**.

Kriptografske **funkcije sažetka** (engl. *hash*) treća se vrsta kriptografskog algoritma i koriste se za provjeru autentičnosti podataka dohvaćenih iz nepouzdanog izvora ili za dodavanje sloja sigurnosti. Uzimaju poruku bilo koje duljine kao ulaz i daju sažetak fiksne duljine, koji se može koristiti u, među ostalim, digitalnom potpisu [4]. Za dobre funkcije sažetka, napadač ne može pronaći dvije poruke koje proizvode isti sažetak. **MD4** je dugo korištena funkcija sažetka koja je sada razbijena, kao i njezina ojačana varijanta **MD5** te se smatraju potpuno nesigurnima. Američka agencija za nacionalnu sigurnost razvila je seriju MD5 funkcija raspršivanja [7].

2.2.2. Asimetrična kriptografija

Asimetrična kriptografija poznata je i kao sustav kriptiranja javnim ključem. Šifriranje simetričnim ključem koristi isti ključ za šifriranje i dešifriranje poruke. Značajan nedostatak simetričnih šifri je to što svaki odvojeni par strana u komunikaciji mora dijeliti drugačiji ključ, a broj potrebnih ključeva raste kao kvadrat broja članova mreže što vrlo brzo zahtijeva složene sheme upravljanja ključevima kako bi svi ostali dosljedni i tajni [4]. Slika 2.2 prikazuje princip šifriranja čistog teksta i dekripcije šifrata različitim ključem iz čega se ponovno dobiva čisti tekst.



Slika 2.2: Princip rada asimetrične šifre, slika preuzeta iz [9]

1976. godine predložen je pojam kriptografije s javnim odnosno asimetričnim ključem gdje se koriste dva različita, ali matematički povezana ključa, **javni ključ** i **privatni ključ**. Izračunavanje jednog iz drugog nije moguće, iako su nužno povezani. Umjesto toga, oba se ključa generiraju tajno, kao međusobno povezani par. U takvim sustavima javni ključ, koji se koristi za šifriranje, može se slobodno dijeliti, dok njegov

upareni privatni ključ, koji se koristi za dešifriranje, mora ostati tajna. **Algoritam RSA** zasnovan je na teoriji brojeva, a temelji se na problemu faktorizacije. RSA smatramo jednim od najjačih algoritama, no i dalje nije u potpunosti otporan na probijanje [10]. Osim RSA, postoje neka od poznatih rješenja koja se temelje na teoriji kodiranja i teoriji brojeva, dok je sigurnost povezana s problemom dekodiranja općenitog linearnog koda i problemom diskretnog algoritma [7].

Kriptografija javnim ključem također se koristi za implementaciju shema digitalnog potpisa. **Digitalni potpis** podsjeća na obični potpis, korisnik ga lako napravi, ali ga je bilo kome drugome teško krivotvoriti [4]. Digitalni potpisi također mogu biti trajno vezani za sadržaj poruke koja se potpisuje i tako garantiraju integritet dokumenta. U shemama digitalnog potpisa postoje dva algoritma: jedan za potpisivanje (koristi tajni ključ, sažetak poruke ili oboje) te jedan za provjeru (koristi odgovarajući javni ključ s porukom da provjeri valjanost potpisa). Svatko može provjeriti ispravnost digitalnog potpisa ako ima na raspolaganju javni ključ potpisnika. RSA i DSA dvije su najpopularnije sheme digitalnog potpisa. Za optimizaciju digitalnog potpisa koriste se funkcije sažetka bez kojih bi potpis bio iste veličine kao i poruka [11].

3. Opis pokazne igre

Ovo poglavlje opisuje konceptualni dizajn igre pri čemu se daje osvrt na cilj igre, način na koji se mehanike unutar igre koriste i ambijent igre.

3.1. Cilj igre

Igrač, pomoću tematski oblikovanih uputa, saznaje da mu vještica, koja je ujedno i njegova učiteljica, želi prenijeti svoje znanje o stvaranju napitaka. Kako obični ljudi ne bi mogli lako saznati vještičje tajne, recepti napitaka kriptirani se pomoću različitih šifri klasične kriptografije. Igračeva zadaća dešifriranje je sva četiri recepta i otkrivanje svih tajnih napitaka. U igri nije moguće ostvariti neuspjeh te su jedina mjerila uspješnosti količina otkrivenih napitaka i dosezanje zadnje razine igre. Na taj se način veći naglasak stavlja na edukativnu funkciju igre, kako bi igrač svojim tempom mogao savladati ponuđene tehnike šifriranja i dešifriranja.

3.2. Mehanika igre

Igra je dizajnirana s naglaskom na edukativni sadržaj vezan uz područje kriptografije. Zbog toga, mehanike igre su jednostavne i intuitivne te ne kažnjavaju igrača. Shodno jednostavnosti odabranih mehanika, igra je pristupačna velikom broju ljudi. S obzirom na to da je riječ o računalnoj igri, unos se ostvaruje tipkovnicom i mišem, a prilikom korištenja miša, igrač se služi trima tehnikama:

1. **Prelazak mišem preko predmeta** (eng. *hover*) – prilikom prelaska mišem preko određenih objekata u igri, igraču se prikazuje detaljni opis objekta;

2. **Klik na predmet** – pomoću jednostrukog lijevog klika mišem na neki predmet uspostavlja se interakcija s tim predmetom. Primjerice, ako korisnik klikne na papirić za poruke, otvara se tekstualni okvir koji prikazuje vještičju poruku;

3. **Povlačenje i ispuštanje pomoću tipke miša** (eng. *drag-and-drop*) – kada se kursor miša nalazi direktno iznad sastojka koji igrač želi koristiti prilikom stvaranja novog recepta, lijevim klikom miša se taj sastojak odabire te se, ne ispuštajući lijevi klik, prenosi iznad objekta predodređenog za miješanje sastojaka (čarobni kotao) i otpušta. Ako je predmet pušten prije nego se nalazi iznad kotla, njegova se pozicija postavlja na početnu (prije akcije povlačenja).

Svaki put kad igrač uspješno napravi novi napitak, odnosno uspije dešifrirati vještičju poruku, nagrađen je animacijom predstavljanja novog napitka. Ako igrač ubaci krive sastojke, animacija će prikazivati eksploziju sastojaka.

3.3. Ambijent

Osim grafičkih elemenata, ostvarenju ambijenta igre doprinose i auditivni sadržaji. Mjesto radnje radna je soba vještice slična tamnici (kameni zidovi i pod), a pozornost igrača usmjerena je na veliki drveni stol popunjen sastojcima. Zajedno s elementima igre s kojima igrač ne može stupiti u interakciju, sastojci i pomagala na raspolaganju igraču doprinose mističnom ugođaju igre. Zvuk igre, sačinjen od ambijentalne glazbe te zvukova kamina i grmljavine u pozadini, doprinosi smirujućem ugođaju, kako bi se igrač mogao bez pritiska koncentrirati na kriptografske probleme koje mu je zadala vještica.

3.4. Dizajn igre

Igra je namijenjena za jednog igrača (engl. *Single-player*), a žanr je igra zagonetke (engl. *puzzle game*). Svi grafički materijali izrađeni su samostalno u pikseliziranoj 2D tehnici (engl. *pixel art*). Igrač na raspolaganju ima kristalnu kuglu pomoću koje može detaljno proučiti vrstu šifriranja koja se koristi za trenutnu razinu igre. Također, prilikom korištenja tehnike prelaska mišem preko predmeta, igrač može pročitati detaljne opise sastojaka pomoću kojih će uspješno dešifrirati recepte i napraviti odgovarajući napitak. Igrač se može koristiti i bilježnicom za zapisivanje svojih misli. Igra ima četiri razine, a zadaća igrača uspješno je dešifriranje svih recepata te ubacivanje ispravnih sastojaka u kotao kako bi prešao na iduću razinu. U razinama igre koriste se sljedeće šifre:

1. **Cezarova šifra** (engl. *Caesar Cipher*),

2. **Playfairova šifra** (engl. *Playfair Cipher*),

3. **Šifra željezničke ograde** (engl. *Rail Fence Cipher*) i

4. **Šifra stupčaste transpozicije** (engl. *Columnar Transposition Cipher*).

Šifriranje Cezarovim kodom temelji se na pomaku abecede i radi se o jedno-abecednoj supstitucijskoj šifri, tj. isto slovo zamjenjuje se samo jednim drugim (uvijek isto za zadanu šifriranu poruku). [12].

Playfairova šifra koristi tehniku ručne simetrične enkripcije. Simetrična enkripcija znači da se isti ključ koristi za šifriranje i dešifriranje poruka. Tehnika šifrira parove slova, umjesto pojedinačnih slova kao u jednostavnoj supstitucijskoj šifri [13].

Šifra željezničke ograde klasična je vrsta transpozicijske šifre. Ime je dobila po načinu na koji se šifriranje izvodi. Transpozicijska šifra je metoda šifriranja pomoću koje se pozicije koje zauzimaju jedinice originalnog teksta (koje su obično znakovi ili skupine znakova) pomiču u skladu s nekim pravilom, tako da šifrirani tekst čini permutaciju originalnog teksta. Jednostavnije, promijenjen je redoslijed znakova originalnog teksta [14]. Prednost šifre željezničke ograde nad ostalim transpozicijskim šiframa je da postoji promjenjiva udaljenost između uzastopnih slova [15]. Šifra stupčaste transpozicije također je oblik transpozicijske šifre te uključuje ispis originalnog teksta u redove, a zatim čitanje šifriranog teksta u stupcima jedan po jedan.

4. Razvoj pokazne igre

Sukladno konceptima koji su ranije opisani, ovo poglavlje daje detaljniji osvrt na konkretnu implementaciju pokazne igre. Implementacija je tematski podijeljena u dva dijela pri čemu je u prvom dijelu opisana izrada glavnog izbornika, koji je ujedno i početna scena, dok je u drugom dijelu prikazana izrada glavne scene sa svim elementima igre i pripadajućim mehanikama. Svi grafički elementi izrađeni su samostalno, a za ostvarenje programskog rješenja korištena je razvojna okolina **Unity** sa skriptama pisanim u programskom jeziku **C#**.

4.1. Razvojna okolina Unity

Razvojna okolina Unity prikladna je za razvoj više-platformskih igara što, osim računalnih igara, uključuje i konzolne te razne oblike simulacija. Funkcionalnosti igre ili simulacije izrađene unutar Unityja ostvaruju se dodavanjem objekata na scenu te opisivanjem njihovog željenog ponašanja unutar nekog integriranog razvojnog okruženja za oblikovanje koda. U ovom slučaju, za uređivanje koda se koristi *Microsoft Visual Studio*, a korištena inačica Unityja je 2020.3.18.f1 Personal.

4.2. Izrada glavnog izbornika

Glavni izbornik ostvaren je kao skupina tipki za pokretanje nove ili postojeće igre, otvaranje podizbornika za opcije igre, prikaz informacija o autorima igre te izlazak iz igre. Navigacija takvim izbornikom implementirana je eksplicitnim odabirom redoslijeda kojim se mijenja fokus trenutne tipke pritiskom na strelice ili na "W" i "S". Slika 4.1 prikazuje raspored tipki za navigaciju te grafičku pozadinu na kojoj se oni nalaze.

Slika 4.1: Raspored elemenata glavnog izbornika

Pritiskom na tipku "New Game" pokreće se nova igra bez učitavanja spremljenog napretka, a takva funkcionalnost opisana je metodom "OpenNewGame" unutar skripte "NewGameButton" (Programski isječak 4.2).

```
1       public class NewGameButton : MonoBehaviour
2       {
3           public void OpenNewGame()
4           {
5               PlayerPrefs.SetInt("Level", 1);
6               PlayerPrefs.SetInt("NewGameButtonPressed", 1);
7               GameObject.FindGameObjectWithTag("closingPanel").GetComponent<
    Animator>().Play("ClosePanelMenu", -1, 0f);
8               Invoke("ChangeScene", 2f);
9           }
10      }
11
```

Programski isječak 4.2: Funkcija "OpenNewGame" iz skripte "NewGameButton" koja ostvaruje izmjenu scene

Izbornik za promjenu postavki igre odnosi se isključivo na postavke vezane za zvuk (Slika 4.3), a spremanje stanja igre, koje se propagira u sljedeće pokretanje, ostvareno je korištenjem klase *"PlayerPrefs"* koja pohranjuje podatke u obliku tekstualnih i/ili brojčanih vrijednosti.

Slika 4.3: Podizbornik za postavke zvuka

Primjer spremanja podataka prikazan je unutar isječka skripte "MenuVolumeScript" (Programski isječak 4.4), a ista se tehnika koristi i za spremanje stanja unutar glavne scene.

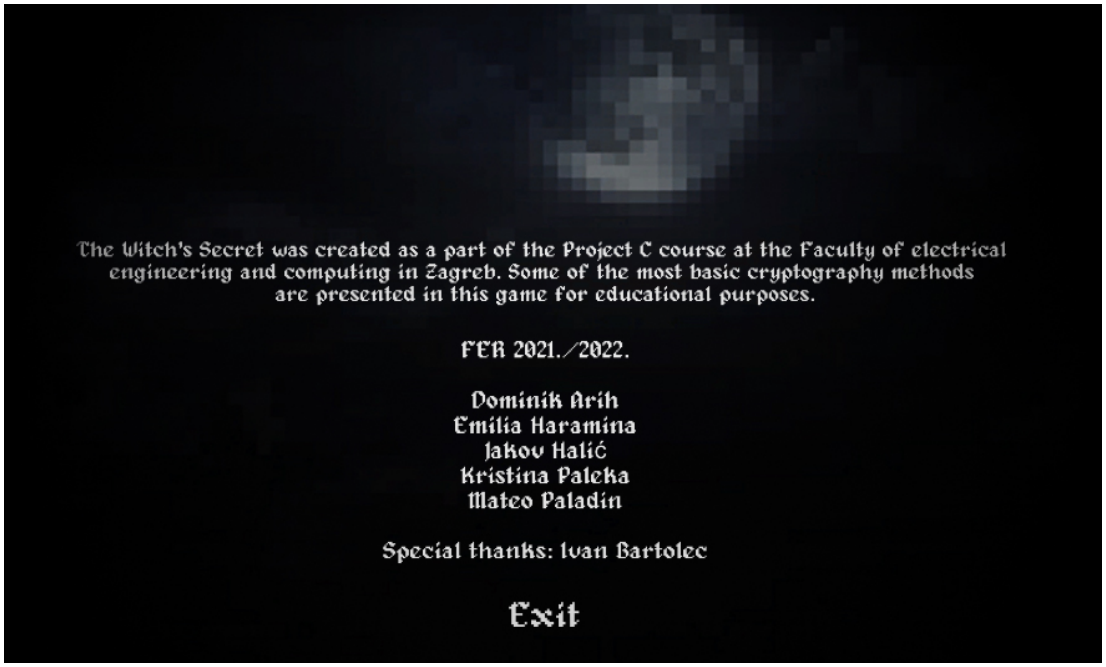
```
        public void MusicButtonPress()
        {
            if (PlayerPrefs.GetInt("Music") == 0)
            {
                musicOn.gameObject.GetComponent<Text>().text = "Off";
                PlayerPrefs.SetInt("Music", 1);
            }
            else if (PlayerPrefs.GetInt("Music") == 1)
            {
                musicOn.gameObject.GetComponent<Text>().text = "On";
                PlayerPrefs.SetInt("Music", 0);
            }
        }

        public void SfxButtonPress()
        {
            if (PlayerPrefs.GetInt("SFX") == 0)
            {
                sfxOn.gameObject.GetComponent<Text>().text = "Off";
                PlayerPrefs.SetInt("SFX", 1);
            }
            else if (PlayerPrefs.GetInt("SFX") == 1)
            {
                sfxOn.gameObject.GetComponent<Text>().text = "On";
                PlayerPrefs.SetInt("SFX", 0);
            }
        }

```

Programski isječak 4.4: Funkcije "MusicButtonPress" i "SfxButtonPress" mijenjaju staro i pohranjuju novo stanje u kojem se određeni element nalazi

Odabirom tipke "About" otvara se prikaz informacija o autorima igre (Slika 4.5), a pritiskom na "Exit" igra se gasi. Gašenje igre ne uzrokuje gubitak spremljenih podataka zato što su oni ažurirani za vrijeme trajanja igre, a ne po izlasku iz scene.

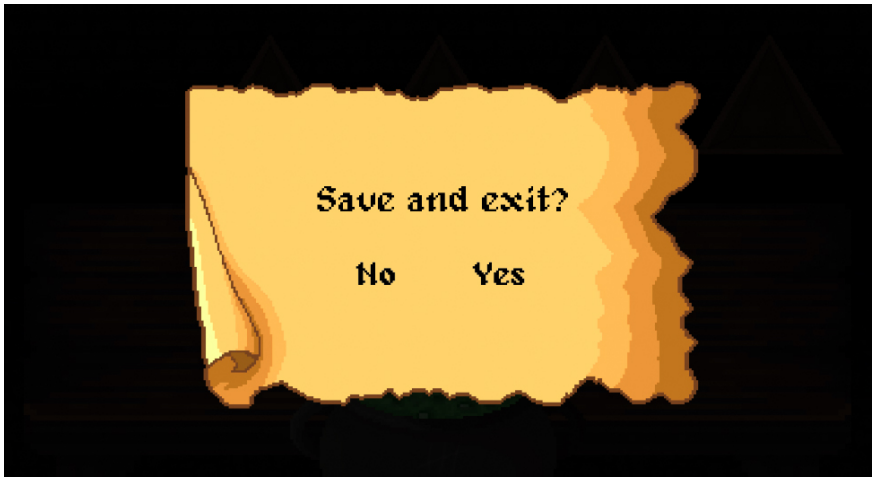


Slika 4.5: Prikaz podataka o autorima igre

4.3. Izrada glavne scene

Unutar glavne scene smješteni su elementi igre povezani interaktivnim mehanikama koje igraču omogućuju ispunjavanje pretpostavljenih zadataka. Pri pokretanju igre, elementi scene su učitani shodno spremljenom napretku igrača provjerom vrijednosti unutar klase *"PlayerPrefs"* (kao što je opisano u ranijim poglavljima).

Glavna scena povezana je s glavnim izbornikom. Pritiskom na tipku "Esc" igraču se nudi opcija spremanja trenutnog napretka i povratka na izbornik ili nastavka igre (Slika 4.6), a interakcija s drugim elementima privremeno je onemogućena. Odabirom opcije "Yes" dešava se odgođena tranzicija između dviju scena, a odabirom opcije "No" izbornik se zatvara i igraču je ponovno omogućena interakcija s elementima.



Slika 4.6: Izbornik koji se otvara pritiskom na tipku "Esc"

4.3.1. Interaktivni elementi i mehanika igre

Na scenu je postavljena statična pozadina koju čine kameni zid i drveni stol. Interaktivni elementi nalaze se na stolu u obliku sastojaka i čarobne kugle ili ispred stola u obliku bilježnice i čarobnog kotla. Elementi koje nije moguće izravno koristiti za izvršavanje zadataka nalaze se na zidu: police za novootkrivene napitke i sat čije kazaljke pokazuju brojeve potrebne za rješavanje jedne od zagonetki. Objekte je bilo potrebno rasporediti tako da ni u kojem trenutku jedan drugoga ne prekrivaju kako se ne bi onemogućila interakcija s prekrivenim objektima. Konačan raspored elemenata scene prikazana je na slici 4.7.

Slika 4.7: Konačan raspored elemenata glavne scene

Većinska interakcija s elementima uključuje jednostavnu ***"Point and click"*** mehaniku gdje igrač pokazivačem miša prekriva predmet koji želi odabrati te jednostrukim klikom izvršava akciju odabira. Svaki element koji je moguće tako odabrati sadržava komponentu "Button" i pripadajuću metodu "OnMouseDown" koja izvršava željenu akciju. Programski isječak 4.8 prikazuje izvršavanje metode "OnMouseDown" na zidnom satu prilikom čega se svira određeni zvuk.

```
1      public class ClockSound : MonoBehaviour
2        {
3             void OnMouseDown()
4            {
5                if (OpenNote.noteOpened == false && Notebook.notebookOpened == false)
6                SoundManagerScript.PlaySound("clock");
7             }
8        }
9
```

Programski isječak 4.8: Metoda "OnMouseDown" zidnog sata svira zvuk prilikom jednostrukog klika na objekt

Svakom sastojku pridružen je pripadajući opis koji se prikazuje korištenjem ***"On hover"*** odnosno ***"On mouse over"*** mehanike. Kada se kursor miša nalazi direktno iznad sastojka, otvara se mali dijaloški okvir koji nudi informacije o imenu i namjeni tog sastojka. Slika 4.9 prikazuje pojavljivanje dijaloškog okvira za sastojak "Wolfsbane", a programski isječak 4.10 sadrži dijelove skripte "ShowDescription" koji ostvaruju navedenu funkcionalnost.

Slika 4.9: Prikaz opisa sastojka "Wolfsbane"

```
    public class ShowDescription : MonoBehaviour
      {
          public GameObject description;
          public static bool clickedObject;
          void OnMouseOver()
          {
              if (clickedObject == false)
              {
                  if (OpenNote.noteOpened == false && Notebook.noteBookOpened ==
  false)
                  {
                      description.SetActive(true);
                  }
              }
              else
              {
                  description.SetActive(false);
              }
          }
          void OnMouseExit()
          {
              description.SetActive(false);
          }
          void OnMouseDown()
          {
              clickedObject = true;
              description.SetActive(false);
          }
          void OnMouseUp()
          {
              Invoke("changeBolleanValue", 0.5f);
              if (description.activeInHierarchy)
              {
                  description.SetActive(false);
              }
          }
      }

```

Programski isječak 4.10: Metode skripte "ShowDescription" zadužene za prikaz dijaloškog okvira elementa

Najvažnija mehanika koju igru koristi upravo je ***"Drag and drop"*** mehanika. Po pritisku i zadržavanju lijevog klika miša na sastojku, igraču je omogućeno pomicanje sastojka u smjeru pomicanja kursora miša. Na taj način igrač može dodavati sastojke u kotao otpuštajući pritisak miša kada se objekt nalazi iznad kotla. Prilikom otpuštanja pritiska kada objekt nije iznad kotla, objekt se vraća na svoju početnu poziciju. Moguće je nositi najviše jedan sastojak odjednom. Za ostvarenje takve funkcionalnosti objektima je pridružena skripta koja sardži metode prikazane u programskom isječku 4.11.

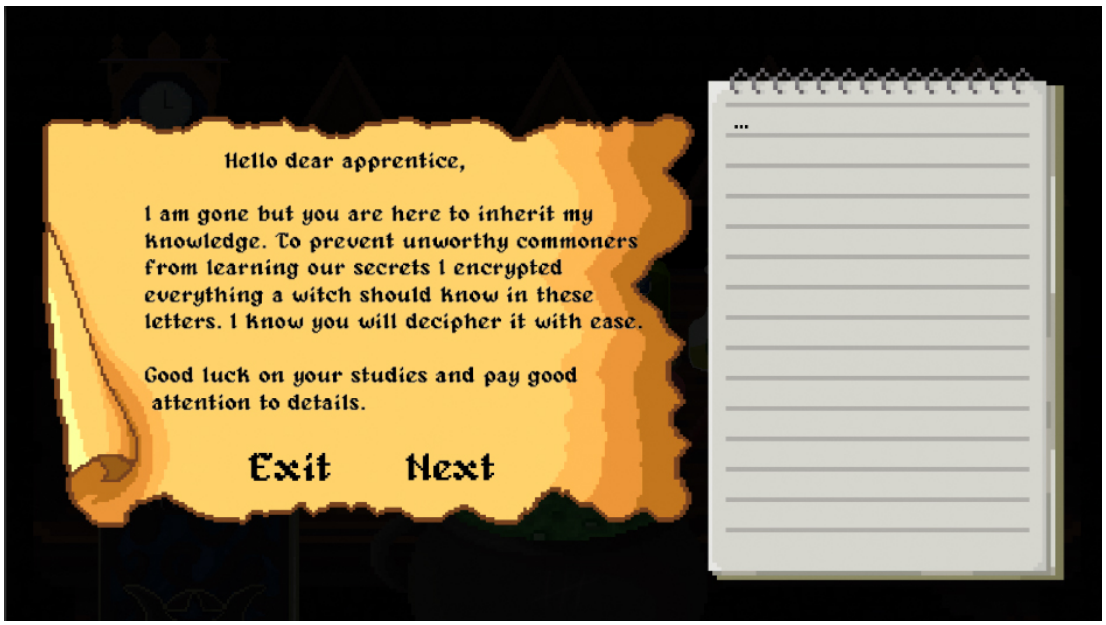
```
1       void Update()
2        {
3            if (placed) return;
4            if (!dragging) return;
5            Vector2 mousePosition = new Vector3();
6            mousePosition = GetMousePos();
7            transform.position = mousePosition - offset;
8        }
9         void OnMouseDown()
10       {
11           if (OpenNote.noteOpened == false && Notebook.noteBookOpened == false)
12           {
13               dragging = true;
14               offset = GetMousePos() - (Vector2)transform.position;
15           }
16
17       }
18       void OnMouseUp()
19       {
20           if (Vector2.Distance(transform.position, GameObject.FindGameObjectWithTag
    ("cauldron").gameObject.transform.position) < 2)
21           {
22               transform.position = GameObject.FindGameObjectWithTag("slot").
    gameObject.transform.position;
23               placed = true;
24               CauldronSlot.objectsInCauldron++;
25               CauldronSlot.objects.Add("SeaHolly");
26           }
27           else
28           {
29               transform.position = originalPosition;
30               dragging = false;
31           }
32       }
33
```

Programski isječak 4.11: Metode "OnMouseUp" i "OnMouseDown" omogućuju nošenje i otpuštanje sastojaka

Potrebno je detaljnije objasniti načine na koje interaktivni elementi koriste opisane mehanike kako bi igrač takvim elementima mogao manipulirati i igru dovesti u željeno stanje (dobivanje nagrade). U tu svrhu osvrnut ćemo se na četiri objekta: papirić za poruke, bilježnicu, čarobna kuglu i kotao.

Papirić za poruke

Na sredini stola nalazi se papirić koji svjetluca kada se na njemu nalazi poruka koju igrač još nije pročitao. Za svaku razinu (svaki napitak), pritiskom na objekt prikazuje se jedinstvena poruka koja igrača uvodi u novu zagonetku. Slika 4.12 prikazuje početni tekst koji je predstavljen igraču prilikom prvog igranja.



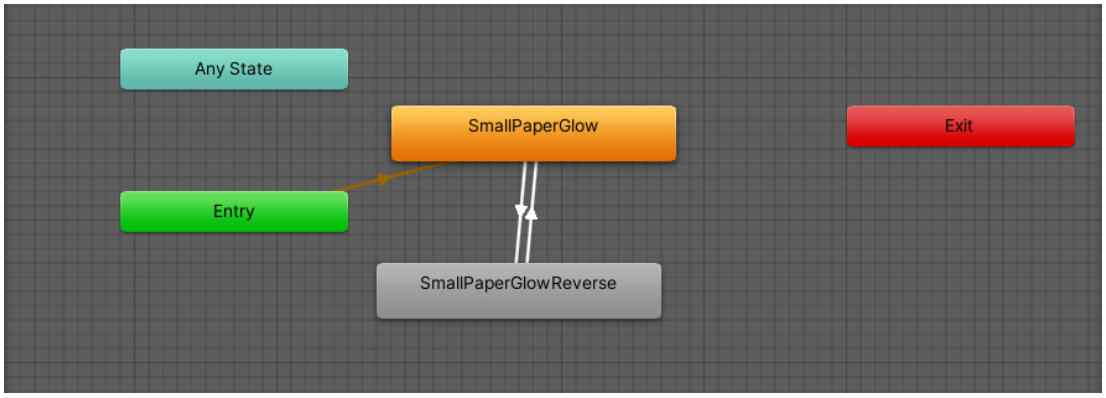
Slika 4.12: Jedan od tekstova koji igrača upućuju u novu zagonetku

Navigacijskim tipkama "Next" i "Exit" igrač prelazi na preostale dijelove teksta koji opisuje zagonetku ili izlazi iz prikaza poruke. Programski isječak 4.13 prikazuje jednostavno iteriranje dijelovima teksta pritiskom na "Next".

```
1        public void Next()
2        {
3            SoundManagerScript.PlaySound("paper");
4            if (TextIndexes.activeIndex < 2)
5            {
6                TextIndexes.activeIndex++;
7            }
8            else if (TextIndexes.activeIndex == 2)
9            {
10               TextIndexes.activeIndex = 0;
11           }
12       }
13
```

Programski isječak 4.13: Metoda "Next" koja učitava idući dio poruke papirića

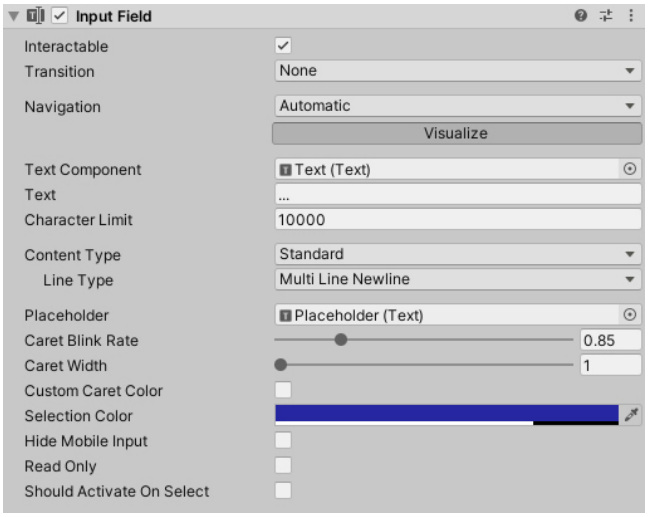
Svjetlucanje papirića ostvareno je korištenjem animacijskog sustava koji nasumično izmjenjuje stanja slabijeg ili jačeg osvjetljenja objekta (Slika 4.14).



Slika 4.14: Animacije koje kontroliraju intenzitet osvjetljenja papirića

Bilježnica

Na slici 4.12, s desne strane poruke igraču, vidljiv je prikaz bilježnice unutar koje igrač može unositi svoje bilješke pritiskom na prazni redak i unosom pomoću tipkovnice. Bilježnicu je moguće otvoriti i pritiskom na pripadajući objekt u donjem lijevom uglu scene (Slika 4.7), a slika 4.15 prikazuje postavke komponente "Input Field", pridružene objektu bilježnice, unutar koje se sprema tekst upisan u bilježnicu.



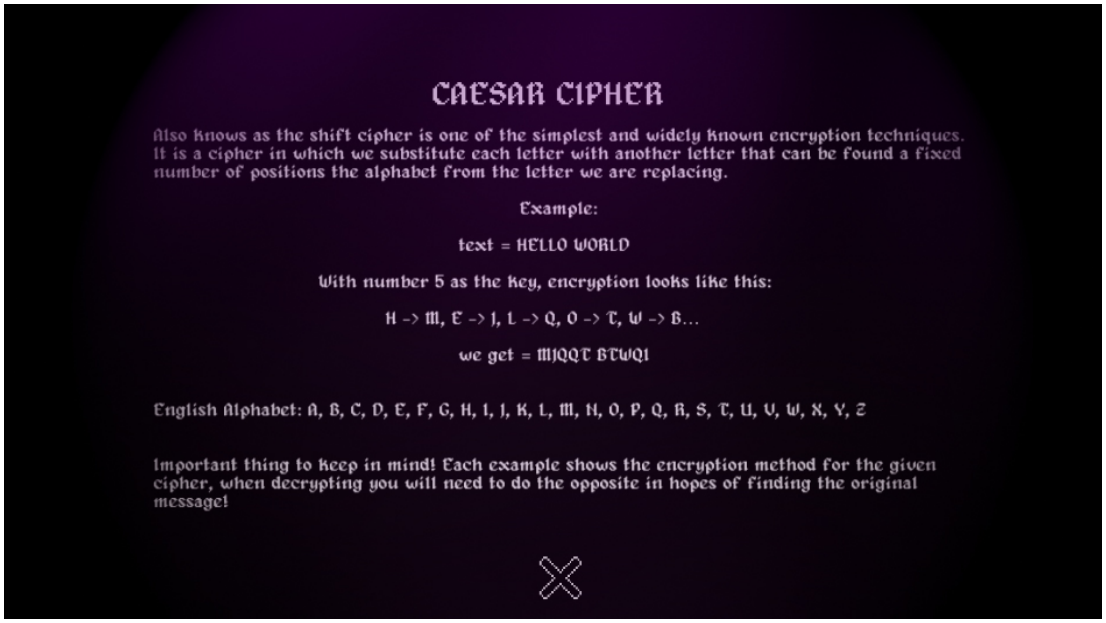
Slika 4.15: Postavke komponente "Input Field" pridružene objektu bilježnice

Čarobna kugla

Pritiskom na čarobnu kuglu koja se nalazi u donjem desnom uglu scene (Slika 4.7) izvršava se animacija "ulaska u kuglu" prilikom čega se kamera fokusira na objekt i smanjuje svoje vidno polje (engl. *Field of view*) iznad objekta kako bi se ostvario željeni efekt. Po završetku animacije, pojavljuje se prikaz unutrašnjosti kugle.

Unutrašnjost kugle predstavljena je opisom tehnike šifriranja vezane uz razinu na kojoj se igrač u tom trenutku nalazi. Igrač u bilo kojem trenutku iz kugle može izaći pritiskom na tipku koja se nalazi u donjem središnjem dijelu scene (Slika 4.16) prilikom čega se ponovno izvršava prethodna animacija obrnutim redoslijedom.

Kako bi se ostvario željeni ambijent i osjećaj mističnosti, unutrašnjost kugle dočarana je ljubičastim nijansama preko kojih se pružaju dinamične zrake svjetlosti. Slika 4.16 prikazuje opisane elemente obavijene **"Vignette"** efektom u svrhu dočaravanja oblika kugle.



Slika 4.16: Prikaz teksta unutar kugle na prvoj razini igre

Čarobni kotao

Ranije je spomenuto da se prilikom otpuštanja sastojka iznad kotla on dodaje u kotao. U jednom trenutku kotao može sadržavati maksimalno četiri sastojka, a indikator trenutnog broja sastojaka prikazan je bijelim crtama koje su na njemu označene (Slika 4.7). Prilikom dodavanja sastojaka u kotao kao i nakon evaluacije kombinacije dodanih sastojaka (nakon četvrtog), izvršavaju se pripadajuće animacije koje transformiraju veličinu i položaj objekta. Ako je dodana pogrešna kombinacija, prikazati će se animacije eksplozije (Slika 4.17).

Slika 4.17: Izvršavanje animacije eksplozije nakon pogrešne kombinacije sastojaka

Programski isječak 4.18 prikazuje metodu za evaluaciju kombinacije sastojaka dodanih u kotao te izvršavanje pripadajućih akcija po uspjehu ili neuspjehu.

```
1         public void CheckList()
2         {
3         foreach (string obj in objects)
4         {
5             if (PlayerPrefs.GetInt("Level") == 1)
6             {
7                 if (!(objects.Contains("garum")) || !(objects.Contains("vodka")) ||
    !(objects.Contains("holly"))
8                 || !(objects.Contains("peaches")))
9                 {
10                    if (doOnce == false)
11                    {
12
13                        Debug.Log("WRONG COMBINATION");
14                        SoundManagerScript.PlaySound("wrongIngredients");
15                        GameObject.Find("Cauldron").gameObject.GetComponent<Animator
    >().Play("Success");
16                        Invoke("Explode", 2f);
17                        restartPosition = true;
18                        doOnce = true;
19                    }
20                }
21                else
22                {
23                    if (doOnce == false)
24                    {
25                        if (!oneSound)
26                        {
27                            SoundManagerScript.PlaySound("correctIngredients");
28                            oneSound = true;
29                        }
30                        congratulationsPlaying = true;
31                        Debug.Log("SUCESS");
32                        GameObject.Find("Cauldron").gameObject.GetComponent<Animator
    >().Play("Success");
33                    }
34                }
35            }
36            else if (PlayerPrefs.GetInt("Level") == 2)
37            {
38                if (!(objects.Contains("gin")) || !(objects.Contains("absinthe")) ||
    !(objects.Contains("wormwood"))
39                || !(objects.Contains("fairywings")))
40                {
41                ...
42
```

Programski isječak 4.18: Metoda "CheckList" koja provjerava kombinaciju dodanih sastojaka u odnosu na očekivanu kombinaciju

4.3.2. Sustav za nagrađivanje igrača

Nakon prelaska razine (dešifriranja poruke i dodavanja ispravne kombinacije sastojaka u kotao) izvodi se animacija koja igraču predstavlja novootkriveni napitak. Slika 4.19 prikazuje nagradu nakon prve prijeđene razine odnosno otkrivanje napitka "Love Potion".

Slika 4.19: Poruka igraču nakon otkrivanja napitka "Love Potion"

Ovisno o razini na kojoj se igrač nalazi, napitci se na policama prikazuju kao otključani ili zaključani. Slika 4.20 prikazuje razinu na kojoj igrač treba otkriti četvrti napitak.

Slika 4.20: Prikaz stanja napitaka na četvrtoj razini igre

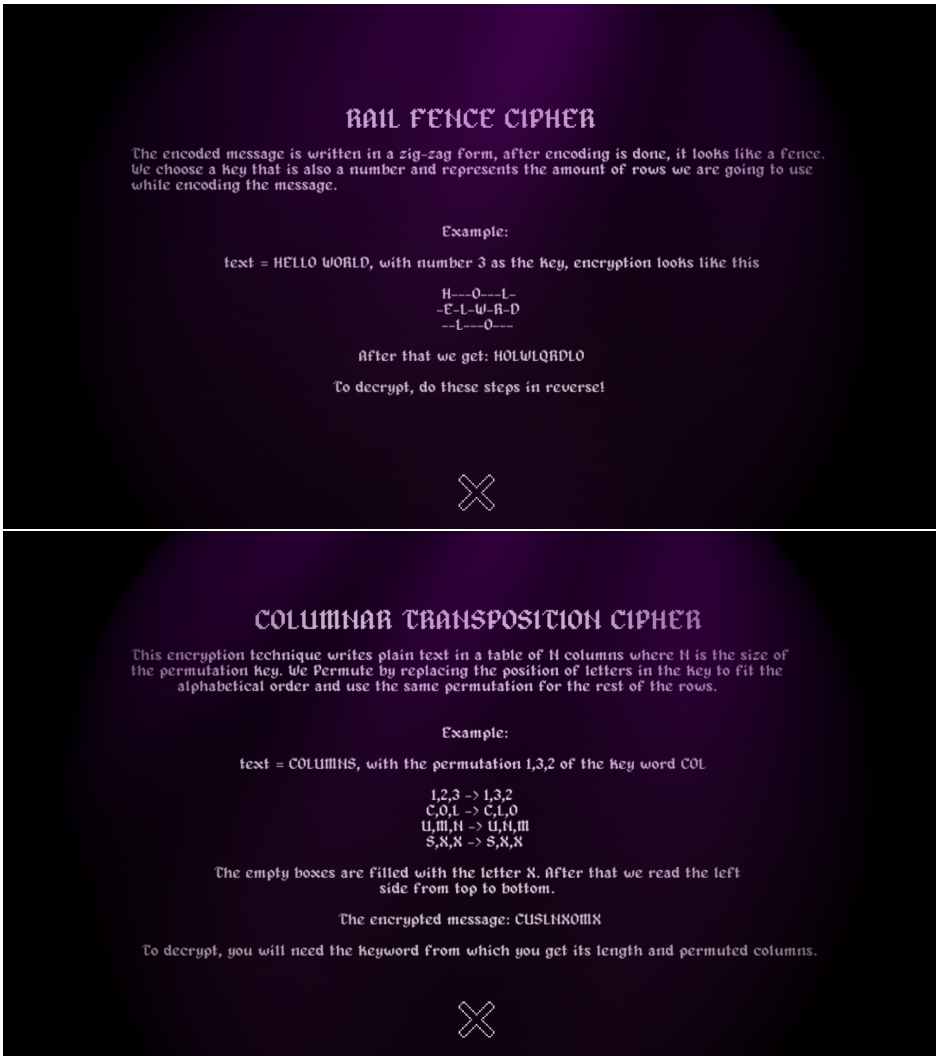
5. Rezultati

Kao rezultat implementacije nastala je pokazna igra "The Witch's Secret" koja je objavljena na poveznici *http://public.tel.fer.hr/witch* u svrhu praćenja broja igrača, vremena igranja, regija iz kojih se igrala i sličnih statističkih podataka. Naredne slike prikazuju slijed događaja za vrijeme jednog igranja.

Klikom na papirić za poruke otvara se tekst zagonetke. Neki od tekstova zagonetki prikazani su na slikama 5.1.

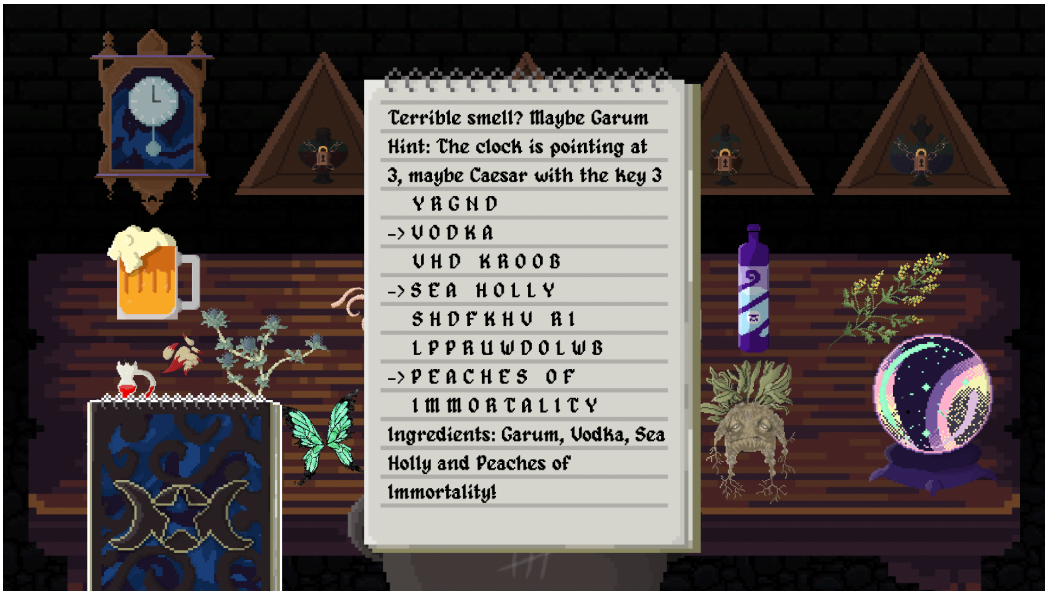
Slike 5.1: Tekstovi zagonetke prve i druge razine

S obzirom na trenutnu razinu, čarobna kugla opisuje različite algoritme šifriranja koja igrač primjenjuje na šifru koja se u tom trenutku nalazi na papiriću (Slike 5.2).



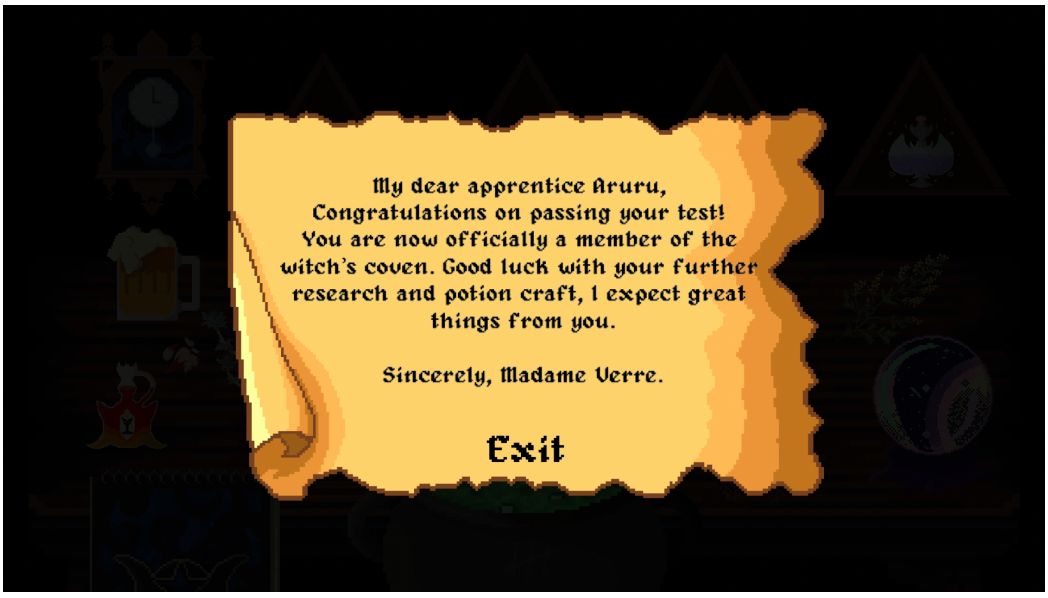
Slike 5.2: Prikaz kugle na trećoj i četvrtoj razini

Tijekom rješavanja zagonetki, igrač vodi bilješke unutar svoje bilježnice kako bi informacije iz čarobne kugle mogao primijeniti na šifru s papirića (Slika 5.3).



Slika 5.3: Bilješke igrača na prvoj razini igre

Nakon što je otključan posljednji napitak, igra je završena i igrač je o kraju igre obaviješten novom porukom na papiriću (Slika 5.4).



Slika 5.4: Tekst vidljiv na papiriću za poruke pri završetku igre

Osim otključanog prvog napitka (Slika 4.19), otključavanje preostalih napitaka prikazano je na slikama 5.5.

Slike 5.5: Poruke dobivene kada igrač u čarobni kotao stavi sastojke svakog od napitaka

6. Zaključak

Izrada obrazovnih videoigara u svrhu učenja novih ili uvježbavanje stečenih vještina odličan je način da se korisnici istovremeno motiviraju i zabave. Uporabom tehnike "dodjele nagrada" za točno izvršene zadatke kao i mogućnošću ponovnog pokretanja zadatka, povećava se želja korisnika za učenjem i olakšava se shvaćanje teme koju igra obrađuje.

U ovom radu opisana je izrada prototipa igre za učenje četiri različite metode šifriranja teksta. Metode šifriranja teksta korisnik uči dešifriranjem poruka koje otkrivaju sastojke napitka, a kasnije, ti isti sastojci dodaju se u kotao u svrhu otkrivanja novih napitaka. Grafički objekti i glazba unutar igre stvaraju mračan i misteriozan ambijent kako bi se korisnik osjećao shodno tematici igre prilikom stvaranja napitaka. Kristalna kugla predstavlja jedan od središnjih i ključnih elemenata igre jer se pomoću nje igraču pruža uvid u detaljna objašnjena za svaku od četiri šifre.

Igra bi se mogla dodatno razviti dodavanjem raznih drugih metodi šifriranja, novih recepata te novih sastojaka. Postoji mogućnost dodavanja nasumičnog generiranja recepata kako bi se postigla mogućnost ponovljivosti unutar igre. Također, kasnije faze razvoja podrazumijevale bi i dodavanje "Easter egg" koncepta koji bi se u ovom slučaju odnosio na otkrivanje napitaka koji nisu dio inicijalnog asortimana igre već su igraču predočeni kao iznenađenje po korištenju neke specifične kombinacije sastojaka. Korištenje takvog koncepta potaknulo bi igrača da više istražuje i eksperimentira kako bi dobio pristup skrivenim elementima igre.

LITERATURA

[1] "Kriptografija - osnovni pojmovi." https://web.math.pmf.unizg.hr/~duje/kript.html. Pristupljeno: 2022-06-26.

[2] "What is cryptoanalysis?." https://www.techopedia.com/definition/1769/cryptanalysis. Pristupljeno: 2022-06-26.

[3] I. A. Al-Kadit, "Origins of cryptology: the Arab contributions," *Cryptologia*, 1992.

[4] G. C. Kessler, "An overview of cryptography," 2003.

[5] J. Fruhlinger, "What is cryptography? How algorithms keep information secret and safe," 2022.

[6] V. B. Liwandouw and A. D. Wowor, "The existence of cryptography: a study on instant messaging," *Procedia Computer Science*, 2017.

[7] "Osnovni pojmovi i uvod u sigurnost." https://www.fer.unizg.hr/predmet/srs_b/materijali#%23!p_rep_122143!_-204120-204121. Pristupljeno: 2022-06-26.

[8] S. M. Abd Ali and H. F. Hasan, "Novel encryption algorithm for securing sensitive information based on feistel cipher," *Test Engeenering Managenment*, 2019.

[9] "Symmetric vs asymmetric: The two types of encryption and how they work." https://sectigostore.com/blog/5-differences-between-symmetric-vs-asymmetric-encryption/. Pristupljeno: 2022-06-27.

[10] E. Milanov, "The RSA algorithm," *RSA laboratories*, 2009.

[11] R. Sobti and G. Geetha, "Cryptographic hash functions: a review," *International Journal of Computer Science Issues (IJCSI)*, 2012.

[12] P. D. S. Limbong, Tonni, “Testing the classic Caesar cipher cryptography using of Matlab,” 2017.

[13] R. Rahim and A. Ikhwan, “Cryptography technique with modular multiplication block cipher and playfair cipher,” 2016.

[14] A. P. U. Siahaan, “Rail-fence-cryptography-in-securing-information,” 2017.

[15] S. Godara, S. Kundu, and R. Kaler, “An improved algorithmic implementation of rail fence cipher,” *International Journal of Future Generation Communication and Networking*, 2018.

PRIMJENA METODA KLASIČNE KRIPTOGRAFIJE NA PRIMJERU EDUKATIVNE IGRE

Sažetak

U svrhu izrade edukativnih materijala na temu klasične kriptografije, ovaj rad opisuje detalje implementacije pokazne igre temeljene na jednostavnim načinima šifriranja. Igrač na raspolaganju ima sve potrebne alate za rješavanje zagonetki koje su mu predstavljene, te je nakon prelaska na novu razinu prikladno nagrađen. Jednostavnost korištenih mehanika i sustav za nagrađivanje igrača osiguravaju optimalnu razinu izazovnosti kako igrač ne bi izgubio koncentraciju. Igra obrađuje tematiku kriptografije kako bi se igrača uputilo u sveprisutnu potrebu za zaštitom informacija i podataka.

Ključne riječi: Pogonski sustav za igre Unity, kriptografija, kriptoanaliza, edukativna igra

APPLICATION OF CLASSICAL CRYPTOGRAPHY METHODS AS PART OF AN EDUCATIONAL GAME

Abstract

For the purpose of creating educational materials on the topic of classical cryptography, this paper describes the details of implementing a game demo based on simple encryption methods. At their disposal, the player has all the tools necessary to solve the presented puzzles and they are appropriately rewarded after advancing to a new level. The simplicity of the used mechanics and the player reward system ensure an optimal challenge level which keeps the player concentrated. The game addresses the topic of cryptography to guide the player into the omnipresent need for protection of information and data.

Keywords: Unity game engine, cryptography, cryptanalysis, educational game