Primjena AES algoritma u sistemima online kupovine

Studentski rad

Vasilije Čabarkapa
Student drugog ciklusa studija
Univerzitet u Istočnom Sarajevu, Elektrotehnički fakultet
Istočno Sarajevo, Bosna i Hercegovina
vascabarkapa@gmail.com

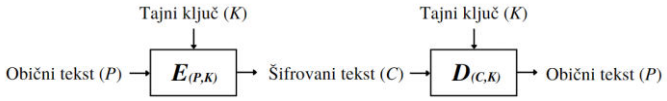
Sažetak — **U informacionom svijetu, vrlo bitan proces predstavlja način zaštite podataka kojim se osiguravaju podaci od oštećenja pri prenosu ili neovlaštenog pristupa. Jedan od najefikasnijih načina zaštite podataka jeste proces enkripcije i dekripcije u kriptografiji, kojim se vrši izmjena podataka, tako da se podaci, ili poruke, čine nečitiljivim za osobe koje ne posjeduju odgovarajući pristupni ključ. Takav princip zaštite podataka može se ostvariti pomoću Naprednog standarda za enkripciju (eng. *Advanced Encryption Standard*, AES). U ovom radu su opisane osnove AES algoritma, proces šifrovanja i dešifrovanja informacija te prednosti i mane upotrebe ovog algoritma. Praktični dio rada prikazuje primjenu AES algoritma na primjeru aplikacije za online kupovinu karata u bioskopu.**

Ključne riječi – AES algoritam; šifrovanje; kriptografija; zaštita podataka; aplikacija;

I. UVOD

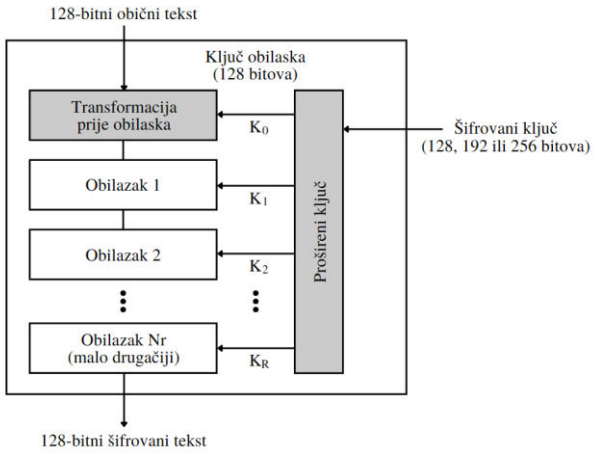
AES enkripcija je tehnologija koja se koristi za šifrovanje elektronskih podataka. Ona koristi 128-bitni, 192-bitni ili 256-bitni simetrični blok algoritam (Sl. 1) za šifrovanje, još poznatiji kao FIPS 197 (eng. *Federal Information Processing Standards*) [1]. Ovaj standard kompjuterske sigurnosti koristi se za zaštitu tajnih i strogo povjerljivih informacija, a objavljuje i održava ga Nacionalni institut za standarde i tehnologiju (eng. *National Institute of Standards and Technology*, NIST).

Algoritam je razvijen od strane Morris Dworkin, Elaine Barker, James Nechvatal, James Foti, Lawrence Bassam, Edward Roback, i James Dray Jr. Objavljen je 26. novembra 2001. godine, a usvojen od strane američke vlade 2002. godine. On je poznat i kao Rijndael algoritam, jer je izveden iz Rijndael porodice algoritama za šifrovanje, koji su razvili belgijski kriptografi Vincent Rijmen i Joan Daemen [1].



Slika 1. Simetrični blok sistem šifrovanja i dešifrovanja [2]

Standard AES enkripcije je implementiran kao zamjena za prethodno korišteni Standard za šifrovanje podataka (eng. *Data Encryption Standard*, DES). U to vrijeme, DES je bio najčešći korišteni metod šifrovanja, ali sa napredovanjem tehnologije i jačinom sajber (eng. *Cyber*) napada, DES je brzo postao laka meta i zastario. Jedan od glavnih problema bila je veličina ključa od samo 56 bitova, što je bilo premalo da bi se spriječilo razbijanje koda. AES je riješio ovaj problem sa većim ključem, što ga čini težim za hakovanje. Oba DES i AES algoritma su šifrovanja blokovskog tipa, što znači da šifruju dijelove podataka, a ne pojedinačne znakove [2]. Grafički prikaz rada AES algoritma prikazan je na Sl. 2. Ovaj metod obezbjeđuje da se identičan tekst šifruje drugačije svaki put kada se pojavi. To daje dodatni nivo zaštite protiv hakera koji pokušavaju pronaći put do dijelova podataka.



Slika 2. Grafički prikaz AES algoritma [2]

Enkripciju putem AES algoritma svakodnevno koriste američke savezne agencije i odeljenja vlade, kao razni nevladini subjekti, komercijalna preduzeća i organizacije, kako bi zaštitili svoje osjetljive podatke. Čak i potrošači, često nesvjesno, koriste uređaje koji implementiraju AES enkripciju (poput Wi-Fi mreža, Google Cloud, Facebook Messenger, Java programiranja itd.). AES je javno dostupan putem NIST-ovog resursnog centra za računarsku bezbjednost i pristup ovoj enkripciji je besplatan [1].

II. IMPLEMENTACIJA

Rijandel je iterativni blok algoritam za šifrovanje, koji omogućava fleksibilnost u pogledu dužine bloka podataka i ključa koji se koriste za šifrovanje. Dužina bloka podataka i ključa može biti 128, 192 ili 256 bitova, nezavisno jedna od druge. Detaljnije informacije o samom procesu šifrovanja i dešifrovanja, kao i specifikacije, mogu se pronaći u zvaničnoj literaturi [3].

A. *Matrica stanja*

Prilikom rada, AES algoritam koristi matricu koja se naziva "matrica stanja" i sastoji se od četiri reda i četiri kolone. Elementi matrice su bajtovi. U sve tri verzije AES-a broj kolona je isti, odnosno sastoji se od četiri 32-bitne riječi. Matrica stanja se koristi kao ulaz i izlaz u AES procesu šifrovanja i dešifrovanja.

Slika 3. Ulazni i izlazni podaci, te matrica stanja

Na Sl. 3 prikazani su ulazni i izlazni podaci sa matricom stanja. Šesnaest ulaznih bajtova $in_0,..,in_{15}$ kopira se u matricu stanja na početku šifrovanja i dešifrovanja. Šifrovanje i dešifrovanje se zatim odvija u matrici stanja i po završetku rezultat se prenese u vidu izlaznih bajtova $out_0,...,out_{15}$.

B. *Ključevi*

Ulazni i izlazni blokovi AES algoritma sadrži blokove podataka dužine 128 bitova i ključeve dužine 128, 192 ili 256 bitova. Dužina ključa biti je predstavljena kao određeni broj 32-bitnih riječi, a u zavisnosti od dužine može biti 4, 6 ili 8 riječi. Broj koraka u algoritmu varira u zavisnosti od dužine ključa, što je prikazano u tabeli 1, koja daje prikaz zavisnosti broja koraka algoritma od dužine ključa, odnosno o implementaciji algoritma (broj koraka i dužina ulaznih/izlaznih blokova dati su u 32-bitnim riječima). Dužina bloka u riječima je označena sa N_w, dužina ključa sa N_k, dok N_r označava broj koraka u algoritmu.

TABELA I. DUŽINE KLJUČEVA, BLOKOVA I BROJ KORAKA U PROCESU AES ALGORITMA [3]

	Nk	**Nw**	**Nr**
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

C. *Šifrovanje*

Šifrovanje podataka putem AES algoritma se sastoji od četiri koraka koji se provode nad oktetima matrice:

1. Zamjena okteta na temelju zamjenske tabele (S-blok);
2. Pomjeranje redova u matrici stanja;
3. Miješanje podataka unutar svake kolone matrice stanja;
4. Dodavanje podključa u matricu stanja.

Algoritam koristi prošireni ključ i prolazi kroz matricu stanja (s) da bi šifrovao ulazni blok (in) i kao rezultat dao šifrovani blok (out) iste dužine kao i ulazni blok. Pseudokod za šifrovanje:

```
početak
   oktet stanje [4, Nw]

   stanje = ulaz
   dodaj_podključ (stanje, w[0, Nw-1])

   za korak=1 do korak=Nr-1 radi
      zamjena_okteta(stanje)
      pomjeranje_redova(stanje)
      mijesanje_kolona(stanje)
      dodaj_podključ(stanje, w[korak*Nw, (korak+1)*Nw-
1])
   kraj

   zamjena_okteta(stanje)
   pomjeranje_redova (stanje)
   mijesanje_kolona(stanje)
   dodaj_podključ(stanje, w[Nr*Nw, (Nr+1)*Nw-1])

   izlaz=stanje
kraj
```

Funkcija *zamjena okteta* je transformacija matrice stanja koja nezavisno radi na svakom bajtu matrice koristeći zamjensku tabelu (S-blok). Bajtovi ulaza se zamjenjuju uz pomoć S-blok tabele i rezultat se čuva u matrici tipa 4x4.

Tokom *pomjeranja redova*, bajtovi u tri zadnja reda matrice stanja se ciklično pomjeraju ulijevo za različit broj pozicija. Prvi red se ne pomjera, drugi se pomjera jednom, treći se pomjera dva puta, a četvrti se pomjera tri puta ulijevo.

Miješanje kolona je funkcija koja mijenja podatke u matrici stanja tako što svaku kolonu množi sa fiksnim polinomom:

$$C(x) = [03]x^3 + [01]x^2 + [01]x + [02]$$

Ova operacija čini poruku komplikovanijom i otežava hakerima da dešifruju istu.

Na kraju, *dodavanje podključa*, odnosno proširenog ključa u matricu stanja se vrši jednostavnom XOR operacijom. To znači da se svaki element matrice stanja povezuje sa odgovarajućim elementom proširenog ključa. Ovo se ponavlja dok se ne dođe do posljednje runde šifrovanja. Rezultat posljednjeg dodavanja proširenog ključa je 128-bitni šifrovani tekst za 128-bitnu običnu poruku.

D. *Prošireni ključ*

Algoritam koristi ključ za šifrovanje K i provodi njegovo proširenje kako bi generisao odgovarajuće podključeve. Proširenjem ključa se generišu 32-bitne riječi. Tačan broj riječi koji se dobije proširenjem se može izračunati pomoću formule $N_w \bullet (N_r + 1)$. Rezultat proširenja je linearni niz 32-bitnih riječi koje se mogu označiti sa w[i], gdje je $0 \leq i < N_w(N_r+1)$. Pseudokod za proširenje ključa:

```
početak
   riječ tmp

   i=0
   dok je i<Nk
      w[i] = riječ(ključ[4+i], ključ[4+i+1],
ključ[4+i+2], ključ[4+i+3])
      i=i+1
   kraj
   i=Nk

   dok je i<Nb*(Nr+1)
      temp = w[i-1]
      ako je (i mod Nk=0)
         temp=zamijeni riječ(rotiraj_riječ(temp)) XOR
Rconst[i]
      inače ako (Nk>6 AND (i mod Nk)=4)
         temp = zamijeni_riječ(temp)
      w[i] = w[i-Nk] XOR temp
      i=i+1
   kraj

kraj
```

Funkcija *zamijeni riječ* prima 32-bitnu riječ kao argument i preoblikuje je primjenom S-bloka na svaki od četiri okteta, a funkcija *rotiraj riječ*, sa druge strane, preuzima riječ u obliku $a_0a_1a_2a_3$ i, kao rezultat rotacije, vraća novu riječ u obliku $a_1a_2a_3a_0$. Konstanta Rconst u zavisnosti od koraka sadrži sljedeću vrijednost: 02^{i-1},00,00,00, gdje indeks i počinje od 1. Pseudokod ukazuje da se prvih N_k riječi proširenog ključa generišu iz glavnog ključa za šifrovanje. Nakon toga, svaka sljedeća riječ w[i] se generiše tako što se izvrši XOR operacija sa prethodnom riječi w[i-1] i riječi N_k pozicija prije w[i-N_k]. Transformacija uključuje rotaciju koja slijedi permutaciju kroz S-blok, te XOR operaciju sa konstantom koraka Rconst[i].

E. Dešifrovanje

Nema velike razlike između procesa šifrovanja i dešifrovanja u AES-u, jer je proces dešifrovanja inverzni proces šifrovanja. Pseudokod za proces dešifrovanja je sličan onome datom za šifrovanje, sa nekoliko izmjena u koracima koji se koriste.

```
početak
   oktet stanje [4, Nw]

   stanje = ulaz
   dodaj_podključ (stanje, w[Nr*Nw, (Nr+1)*Nw-1])

   za korak=Nr-1 do korak=1 radi
      inv_pomjeranje_redova(stanje)
      inv_zamjena_okteta(stanje)
      dodaj_podključ(stanje, w[korak*Nw, (korak+1)*Nw-
1])
      inv_mijesanje_kolona(stanje)
   kraj

   inv_pomjeranje_redova(stanje)
   inv_zamjena_okteta(stanje)
   dodaj_podključ(stanje, w[0, Nb-1])
   inv_mijesanje_kolona(stanje)

   izlaz=stanje
kraj
```

Transformacija *inverzno pomjeranje redova* je inverzna transformacija u odnosu na *pomjeranje redova*. Bajtovi u posljednja tri reda matrice stanja se ciklično pomjeraju za različit broj bajtova udesno, dok se prvi red ne pomjera. *Inverzna zamjena okteta* je inverzna transformacija zamjene bajtova u kojoj se primjenjuje inverzna zamjenska matrica na svaki bajt matrice stanja. *Inverzno miješanje kolona* je takođe inverzna transformacija u odnosu na *miješanje kolona*. Funkcija *dodaj podključ* koja je opisana pri šifrovanju je svoja vlastita inverzija, jer uključuje samo XOR operaciju.

Međutim, AES algoritam takođe podržava drugi način dešifrovanja, koji zadržava isti niz transformacija matrice stanja, ali mijenja redoslijed generisanja podključeva.

Algoritam koji se koristi je izuzetno snažan zbog svoje sposobnosti da generiše međurezultate u svakoj iteraciji bez potrebe za ključem iz prethodne iteracije. Ovaj algoritam se sastoji od tri ključne komponente: nelinerarizacije, linearnog miješanja i dodavanja ključa. Nelinerarizacija onemogućava linearnu korelaciju između ulaza i izlaza, dok linearno miješanje omogućava široku raspodjelu rezultata tokom svake iteracije. Dodavanjem ključa (XOR operacijom) se osigurava otpornost na poznate vrste napada, uključujući linearnu i diferencijalnu kriptoanalizu, poznate (eng. *Known-key*) i povezane (eng. *Related-key*) ključeve napade, interpolacioni napade itd. Algoritam se pokazao kao K-siguran, što znači da nema poznatih načina otkrivanja ključa osim pretraživanjem svih kombinacija [4].

III. SIGURNOST

AES algoritam smatran je boljim i sigurnijim od standarda šifrovanja podataka DES, jer koristi duže ključeve. Duži ključevi su manje podložni napadima, što AES-u daje prednost u poređenju sa DES-om. DES standard šifrovanja podataka bio je ranjiv zbog prekratkog ključa od samo 56 bitova [4], što ga je činilo podložnim napadima grubom silom (eng. *Brutal force*). Napad grubom silom podrazumijeva sistematsko provjeravanje svih mogućih kombinacija ključeva dok se ne pronađe ispravan ključ, što je jedan od načina napada kada nije moguće iskoristiti druge slabosti u sistemu šifrovanja [1]. Ako se datom sistemu da beskonačno mnogo vremena, napadi će u nekom trenutku dati rezultat. Tabela 2. prikazuje broj mogućih kombinacija ključeva koji su izračunati prema formuli 2^n, gdje n predstavlja broj bitova.

TABELA II. ODNOS BROJA MOGUĆIH KOMBINACIJA U ODNOSU NA DUŽINU KLJUČA

Dužina ključa	**Broj mogućih kombinacija**
1 bit	2
2 bita	4
4 bita	16
8 bitova	256
16 bitova	65536
32 bita	$4{,}2 \cdot 10^9$
56 bitova (DES)	$7{,}2 \cdot 10^{16}$
64 bita	$1{,}8 \cdot 10^{19}$
128 bitova (AES)	$3{,}4 \cdot 10^{38}$
192 bita (AES)	$6{,}2 \cdot 10^{57}$
256 bitova (AES)	$1{,}1 \cdot 10^{77}$

Iako se trostruki DES ili 3DES (eng. *Triple DES*) smatra sigurnijim od običnog DES-a, on je i dalje podložan napadima grubom silom u poređenju sa AES-om. Razlika između AES-a i 3DES-a je u tome što AES koristi duže ključeve i brži je u radu. Dužina ključa za šifrovanje 3DES-a je i dalje ograničena na 56 bitova, a u osnovi on je samo algoritam DES koji je primijenjen tri puta na informacije koje se šifruju [1].

Kao što se vidi iz tabele 2, broj mogućih kombinacija ključeva za standardnu verziju AES-a sa 128 bitnim ključem je izuzetno veliki. Na primjer, Frontier superkompjuter [5] može u sekundi da izvede i do 1,102 exaflops, odnosno $1{,}102 \cdot 10^{18}$ flops (eng. *Floating point operations per second*), tj. operacija sa pokretnim zarezom u sekundi. Pretpostavimo da je broj potrebnih flops operacija za provjeru kombinacije ključeva oko 1000, slijedi da je broj kombinacijskih provjera u sekundi

$$(1{,}102 \cdot 10^{18}) / 1000 = 1{,}102 \cdot 10^{15}$$

Pošto jedna godina ima tačno 31536000 sekudni, za probijanje AES-a, koji koristi ključ 128-bitne dužine, neophodno je

$$(3{,}4 \cdot 10^{38}) / [(1{,}102 \cdot 10^{15}) \cdot 31536000] = 9{,}783 \cdot 10^{15}$$

godina. Na osnovu računice, čak i sa superkompjuterom, potrebno bi bilo skoro deset kvadriliona ili milion milijardi godina da se probije 128-bitni AES ključ koristeći napad grube sile. To je više od starosti svemira (13,75 milijardi godina). Ako bi se pretpostavilo da postoji računarski sistem koji bi mogao da probije DES ključ u sekundi, toj istoj mašini bi trebalo čak 149 milijardi godina da razbije 128-bitni AES ključ. Rezultati ostalih maksimalnih vremena za probijanje svih vrsta AES ključeva su data u tabeli 3.

TABELA III. MAKSIMALNO MOGUĆE VRIJEME PROBIJANJA U ODNOSU NA DUŽINU KLJUČA

Dužina ključa	Maksimalno moguće vrijeme probijanja
56 bitova (DES)	65,379 sekundi
128 bitova (AES)	$9{,}783 \cdot 10^{15}$ godina
192 bitova (AES)	$1{,}784 \cdot 10^{35}$ godina
256 bitova (AES)	$3{,}165 \cdot 10^{54}$ godina

Kada bi se AES uspio kompromitovati, posljedice bi bile velike, jer se AES koristi u mnogim važnim aplikacijama. Razlika između AES-128 i AES-256 je minimalna, jer bilo koji napredak koji bi uspio da razbije AES-128, vjerovatno bi uspio i protiv AES-256. AES, kao algoritam, još nikada nije krekovan i siguran je protiv svih poznatih napada grubom silom. Za maksimalnu sigurnost, preporučeno je korištenje ključa veličine koji će biti dovoljno veliki da se ne može razbiti čak ni sa napretkom u brzinama procesora, uzimajući u obzir i Moore-ov zakon o rastu snage računara [6] koji kaže da se snaga računara udvostručuje približno svakih 18-24 mjeseca (ime po Gordon Moore-u, jednom od osnivača Intel-a).

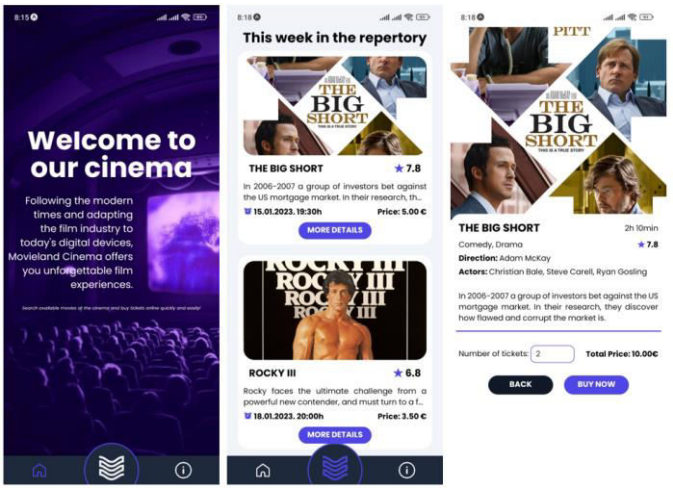
IV. PRIMJENA ALGORITMA

Online kupovina je oblik elektronske trgovine koji omogućava kupcima da direktno kupe proizvode ili usluge od prodavača preko interneta, bilo koristeći web čitač ili mobilnu aplikaciju. Takve prodavnice su fizički ekvivalent kupovine i ovaj proces se često naziva "kupovina od poslodavca do potrošača" (eng. *Business-to-consumer*, B2C). Sistemi za kupovinu preko interneta obično omogućavaju kupcima da pregledaju asortiman proizvoda i usluga kompanije, uključujući informacije o specifikacijama, karakteristikama i cijenama proizvoda.

S obzirom na pandemiju korona virusa COVID-19, posljednjih godina je došlo do značajnog porasta kupovine putem interneta. Međutim, kako se broj kupovina na mreži povećavao, tako je i broj sajber kriminala porastao, što je rezultovalo finansijskim gubicima za žrtve.

Najčešći problemi izazvani online kupovinom predstavljaju nešifrovani podaci. Neke web aplikacije ne šifruju podatke, pa su takvi podaci veoma ranjivi na napade, što predstavlja rizik za kupce koji s tom web lokacijom dijele podatke o kreditnoj kartici i druge osjetljive informacije. Za sigurnu online kupovinu neophodno je preduzeti odgovarajuće mjere opreza. Primjer kupovine pomoću šifrovanja osjetljivih podataka upotrebom AES algoritma dat je u sistemu Movieland Cinema. Kao najduži, 256-bitni ključ obezbjeđuje najjači nivo šifrovanja, pa je shodno tome ova vrsta ključa izabrana za zaštitu podataka u primjeru. Movieland Cinema sistem pruža korisnicima mogućnost da bezbjedno kupuju karte za bioskop upotrebom kreditnih kartica.

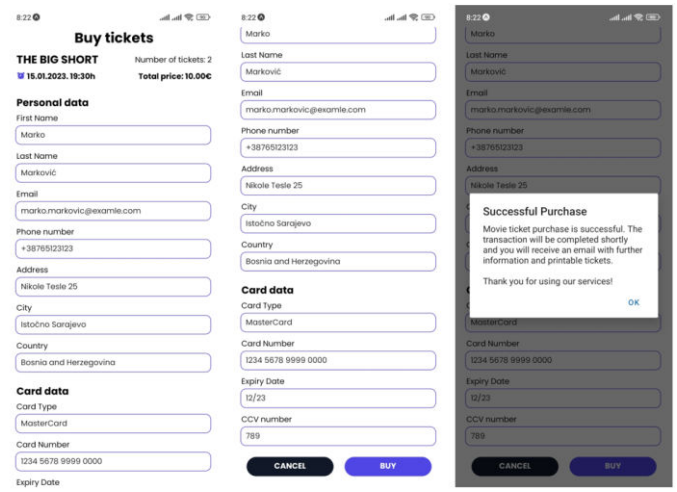
Sistem za kupovinu karata za filmove, Movieland Cinema, se sastoji od dvije aplikacije: admin web aplikacije za upravljanje filmovima, repertoarima i uplatama, te mobilne aplikacije za korisnike preko koje se vrši kupovina karata za filmove koji su dostupni na repertoaru. Glavni fokus sistema je na zaštiti podataka korisnika šifrovanjem putem AES algoritma, kako bi se osigurala sigurnost tokom kupovine karata i da podaci o kreditnim karticama ne budu izloženi zloupotrebi.



Slika 4. Procedura izbora filma u repertoaru

Proces kupovine karata za film počinje u mobilnoj aplikaciji gdje se odabere opcija "*Repertoar*" iz menija u obliku logoa aplikacije (Sl. 4). Korisniku se prikazuju trenutno dostupni filmovi sa kratkim informacijama o nazivu filma, ocjeni, datumu prikazivanja i cijeni pojedinačne karte. Klikom na "*More Details*" učitavaju se detaljnije informacije o filmu,

uključujući kratak opis radnje, režiju, glumce, poster i žanr. Korisnik unosi broj karata koji želi kupiti, a aplikacija automatski izračunava ukupnu cijenu. Nakon unosa, korisnik klikom na "*Buy now*" dugme dolazi do forme (Sl. 5) za unos ličnih podataka (ime, prezime, broj telefona, mejl adresa i adresa stanovanja) i podataka o kreditnoj kartici (vrsta kartice, broj kartice, datum isteka te CCV broj). Potvrdom kupovine pritiskom na "*Buy*" dugme, transakcija se završava.



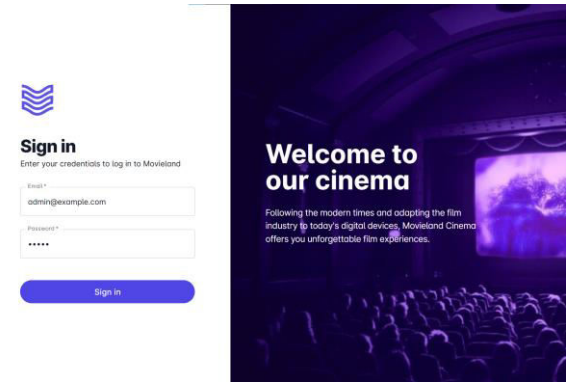
Slika 5. Popunjavanje forme sa potrebnim podacima za kupovinu

Nakon uspješno izvršene transakcije, kupac dobija potvrdu o kupovini na mejl, koja sadrži informacije o kartama za štampanje. Svi podaci o kreditnoj kartici se šifruju prije nego što se skladište na serveru, kako bi bili sigurni od mogućih napada.

Sistem koristi AES-256 enkripciju sa nasumičnim vektorima inicijalizacije. Modul unutar aplikacije generiše nasumični vektor svaki put kada se pozove jedna od metoda šifrovanja. Simetrični ključ može biti bilo koje veličine jer se heširа pomoću SHA-256 (eng. *Secure Hash Algorithm*). U ovom primjeru, kao ključ se koristi mejl adresa korisnika. Prethodno uneseni podaci o kreditnoj kartici se šalju na server, gdje podaci o kartici prolaze kroz AES algoritam i dobijaju novi oblik koji je nečitljiv za oko čovjeka. Primjer skladištenih podataka na serveru poslije izvršavanja algoitma prikazani su na Sl. 6.

```
Purchase tickets
----------------
repertory_id: 2
number_of_tickets: 2
sum_price: 10
first_name: Marko
last_name: Marković
email: marko@example.com
phone_number: +38765123123
address: Nikole Tesle 25
city: Istočno Sarajevo
country: Bosnia and Herzegovina
card_type: U8RFG6aLVZQcTGg8TwWyKftwynfd2csqK44=
card_number: FnYq+HFX+SYHNgAuL3zf9gegBzj4y3MYDwPyN/25xh0=
card_date_expiry: G5XBcr26uwwoLP66bksg8DD9OzZm
card_ccv: u2f6HCQij5jwpcPgGwl6wjcYeg==
date_time_purchase: 2023-01-11 08:37:55
```

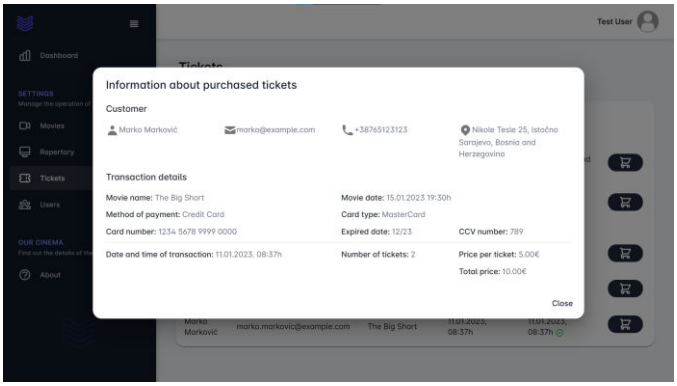
Slika 6. Poslati podaci na server sa šifrovanim podacima o kartici



Slika 7. Prijava na admin web aplikaciji

Vlasnici bioskopa ili drugi ovlašćeni radnici, kao i administratori web aplikacije, mogu da pristupe listi uplata za filmove koje sadrži sve podatke kupaca. Da bi pristupili ovim podacima, oni se moraju prijaviti na sistem (Sl. 7), a zatim odabrati opciju "*Tickets*" iz lijevog menija. Otvara se tabela sa svim uplatama korisnika za filmove. Klikom na dugme sa ikonicom kolica, administratoru se prikazuju detaljne informacije o kupcu i njegovim transakcijama, uključujući datum i vreme uplate. Primjer jednog takvog modala dat je na Sl. 8.

Informacije o karticama korisnika su prikazane u punom formatu kao što su unesene, kao na Sl. 5, iako su skladištene u bazi u šifrovanom obliku. Ovaj oblik skladištenja osigurava privatnost i sigurnost podataka kroz proces dešifrovanja, koji omogućava da se prvobitni oblik podataka vrati u aplikaciju, čime je obezbijeđena sigurnost prilikom slanja i dobavljanja podataka u sistemu.



Slika 8. Podaci o izvršenoj transakciji

Ovaj sistem predstavlja osnovu za dalje razvijanje online kupovine koja nije samo povezana sa bioskopom, već i sa kompanijama koje pružaju širi spektar sadržaja. Pored toga, sistem takođe može da obuhvati i druge načine plaćanja, čiji podaci takođe mogu biti izloženi napadima, kao što je PayPal sistem. Zahvaljujući primjeni AES algoritma, moguće je zaštititi sve vrste podataka koje korisnik smatra da su podložni zloupotrebama.

V. ZAKLJUČAK

Sve je više hakerskih napada na različite vrste računarskih usluga, jer sada većina ljudi provodi puno vremena online - koristeći društvene mreže, e-poštu ili radi preko interneta. Zato je bezbjednost informacija sve važnija kada se razvijaju aplikacije. Znanje o računarskoj sigurnosti i sistemima zaštite postalo je neophodno za povećanje nivoa zaštite i privatnosti korisnika. Implementacijom AES algoritma, korisnici se mogu osjećati sigurnije znajući da su njihovi podaci šifrovani pomoću ovog algoritma.

AES se trenutno smatra jednim od najboljih načina za šifrovanje podataka. Osim što pruža zaštitu, AES takođe nudi nekoliko nivoa sigurnosti, u zavisnosti od potreba korisnika. Za šifrovanje se koriste ključevi dužine 128, 192 ili 256 bitova, što čini algoritam otpornijim na hakovanje. Koncept algoritma je da, bez obzira na nivo vještine i vremena potrebnog za razbijanje enkripcije, treba da bude skuplji od percipirane vrijednosti materijala koji se dešifruje. Nivo zaštite utiče i na performanse sistema, pa je potrebno odlučiti šta je prioritet sistema. Činjenica da ovaj standard koristi američka Agencija za nacionalnu sigurnost (eng. *National Security Agency*, NSA) i mnoge druge institucije, govori o tome koliko je on opšteprihvaćen među razvojnim timovima. Koristi se i u mnogim aplikacijama, kao što su one za bežičnu komunikaciju, finansijske transakcije, elektronska poslovanja, skladištenje šifrovanih podataka itd. Iako se AES za sada smatra neprobojnim, postavlja se pitanje kada će nova tehnologija imati snage da mu se suprostavi.

ZAHVALNICA

Autor se zahvaljuje mentoru doc. dr Nikoli Davidoviću na nesebičnoj pomoći i pruženim savjetima prilikom izrade studentskog rada. Rad je nastao u okviru predmeta Elektronsko poslovanje na drugom ciklusu studija.

LITERATURA

[1] B. Daniel, "What is AES encryption? [The definitive Q&A Guide]", Trusted Computing Innovator, Trenton Systems, Inc, dostupno na: https://www.trentonsystems.com/blog/aes-encryption-your-faqs-answered, posjećeno 03. januara 2023. godine

[2] N. Kaur, N. V. Sai, G. M. Kumar, "Evaulation of DES and AES Cryptographic Algorithms", International Research Journal of Engineering and Technology (IRJET), vol. 8, no. 5, pp. 546-553, maj 2021.

[3] Federal Information, Processing Standards Publication 197, "Advanced Encryption Standard (AES)", National Institute of Standards and Technology, novembar 2001.

[4] A. L. Sousi, D. Yehya, M. Joudi "AES Encryption: Study & Evaluation", CCEE552: Cryptography & Network Security, Rafik Hariri University, novembar 2020.

[5] C. Q. Choi "The beating heart of the world's first exascale supercomputer", IEEE Spectrum, dostupno na: https://spectrum.ieee.org/frontier-exascale-supercomputer, posjećeno 11. januara 2023. godine

[6] E. Mollick, "Establishing Moore's Law", IEEE Annals of the History of Computing, vol. 28, no. 3, pp. 62-75, avgust 2006.

ABSTRACT

In the information world, an essential process is a method of data protection, which ensures data against damage during transmission or unauthorized access. One of the most effective ways to protect data is the process of encryption and decryption in cryptography, which changes data so that data, or messages, become unreadable for people who do not have the appropriate access key. Such a data protection principle can be realized using the Advanced Encryption Standard (AES). This paper describes the basics of the AES algorithm, the process of encryption and decryption of information, and the advantages and disadvantages of using this algorithm. The practical part of the paper shows the application of the AES algorithm with the example of an application for online purchase of cinema tickets.

APPLICATION OF AES ALGORITHM IN ONLINE SHOPPING SYSTEMS

Vasilije Čabarkapa