POBJEDNICI NATJEČAJA CAESAR

Tim: Ivana Dasović, Marta Knežević, Vinko Sabolčec, Karlo Šutalo

Mentor: prof. dr. sc. Marin Golub

NATJEČAJ CAESAR

- Razvoj novih kriptografskih algoritama
- SUPERCOP evaluator
- 3 kategorije:
    - Algoritmi za uređaje s ograničenim resursima
    - Algoritmi za primjenu u uređajima s visokim performansama
    - Algoritmi s dubinskom obranom

REZULTATI PROJEKTA

- Analiza kriptografskih algoritama
- Program za enkriptiranje/ dekriptiranje poruka analiziranim algoritmima
- Web stranica

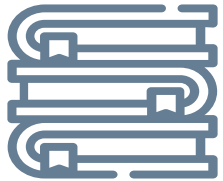
ANALIZA ALGORITAMA

ACORN- 128

- Bitovno orijentiran sekvencijski autentifikacijski algoritam
- Koristi vektor bitova f , vektor *keystream* bitova ks i vektore kontrolnih bitova ca i cb
- Inicijalizacija učitava ključ K i inicijalizacijski vektor IV
- U svakom koraku se provodi generiranje *keystream* bita i *feedback* bita za i-ti korak ks_i te se računa novo stanje
- Šifriranje: u podatkovne bitove m se upisuje nešifrirana poruka te iza nje uzorak od 256 bita koji započinje jedinicom, a svi ostali bitovi su nule (1000...0000)
- Generiranje autentifikacijske oznake T nakon šifriranja

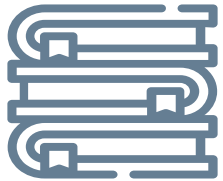
ACORN- 128

- Inicijalizacija ACORN-a je dizajnirana za sprječavanje *linear* napada, *differential* napada i *cube* napada.
- Stanje se ažurira na ne-linearan način- otpornost na klasične napade na šifriranje



AEGIS

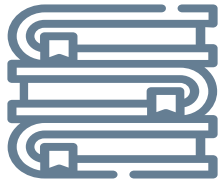
- Koriste AESRound funkciju koja se sastoji od 3 manje funkcije: SubBytes, ShiftRows, MixColumns
- Izvođenje u koracima
  - Inicijalizacija podataka koja služi učitavanju inicijalizacijskog vektora, ključa i konstanti u stanje
  - Određivanje poruke koja se koristi u ažuriranju stanja u i-toj iteraciji inicijalizacije
  - Ažuriranje stanja iteracijama
  - Procesiranje pridruženih podataka
  - Kriptiranje- svaki se blok poruke koristi za ažuriranje stanja i za dobivanje kriptiranog bloka



AEGIS

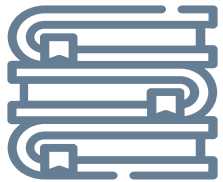
- Generiranje autentifikacijske oznake T
- U svakom koraku funkcija StateUpdate koja služi za ažuriranje stanja
- Ako napadač nije uspio otkriti informacije tijekom *forgery attack*-a, nije moguće razotkriti ključ i stanje brže od iscrpnog pretraživanja ključeva
- Visoka sigurnost i visoke performanse kriptiranja
- 3 podvrste AEGIS algoritma:
  - AEGIS- 128
  - AEGIS- 128L
  - AEGIS- 256

	AEGIS-128	AEGIS-128L	AEGIS-256
Ključ/[bit]	128	128	256
Inicijalizacijski vektor/[bit]	128	128	256
Stanje/[bit]	640	1024	768
Oznaka/[bit]	128	128	128
Maksimalna duljina poruke/[bit]	2^{64}	2^{64}	2^{64}



ASCON

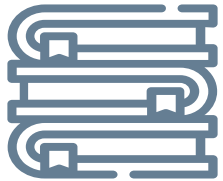
- Familija $\mathrm{ASCON}_{\mathrm{a,b}}$-k-r algoritama za autentificiranu enkripciju
- Pri procesu enkripcije koristi se inicijalizacijski vektor IV koji je specifičan i unaprijed određen za algoritam te se ne koristi tajni broj poruke
- Temelji se na konstrukciji sličnoj MonkeyDuplex, no koristi snažnije funkcije inicijalizacije i finalizacije
- Sastoji se od koraka:
  - Inicijalizacija- početno stanje S od 320 bita formira se pomoću konkateniranja inicijalizacijskog vektora (IV), tajnog ključa i javnog broja poruke
  - Procesiranje asociranih podataka- podatci koji su nastali operacijom *xor* između prvih r bitova stanja S i bloka podataka A_i, te konkatenacijom ostatka stanja S permutiraju se *b* puta



ASCON

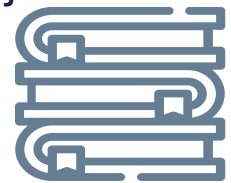
- Enkripcija- blok podataka šifriranog teksta (C_i) određen operacijom *xor* između prvih r bitova stanja S i bloka podataka P_i. Posljednji blok podataka nastao operacijom *xor* se ne permutira b puta
- Dekripcija- operacija *xor* obavlja se između šifriranog teksta i stanja, a rezultat operacije je blok početnog teksta P_i
- Finalizacija- operacija *xor* između stanja S i konkatenacije ključa i znamenki 0, prolazak kroz proces permutacije, xor između izlaza stanja S i ključa K je autentificirajuća oznaka T

- Jednostavna implementacija na hardware-u i software-u uz dobre performance
- Jedan od najbržih algoritama kriptiranja s natječaja CAESAR za kratke poruke



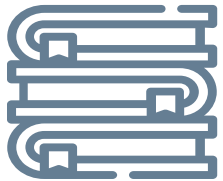
DEOXYS- II- 128

- Jednostavna i razumljiva konstrukcija i implementacija
- Enkripcija:
  - Inicijalizacija- associated data AD i poruke podijelom u blokove od 128 bita i inicijalizacija internog vektora bitova *Auth* na 0
  - Za svaki blok AD_i se računa *Auth* kao *Auth* = *Auth* XOR E_K , u autentifikacijsku oznaku T se stavlja izračunati *Auth i* za svaki blok poruke M_i računa novi T = T XOR E_K i blok šifrirane poruke C_i kao C_i=M_i XOR E_K
- Dekripcija:
  - inicijalizacija- šifrirana poruka C i *associated data* AD podijele se u blokove od 128 bita
  - Dešifriranje analogno šifriranju te se izračunavaju interni vektor *Auth i* autentifikacijska oznaka T'



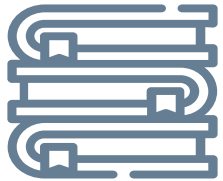
DEOXYS- II- 128

- Ako su izračunate oznake T’ i T jednake vraća se dešifrirana poruka, a u suprotnom se ne vraća ništa
- Deoxys BC je *tweakable block ciper* koji kao parametre prima poruku P, ključ K i parametar *tweak* T
- Vrlo dobre sigurnosne karakteristike
- Efikasan kod kriptiranja malih podataka što je važno kod mnogo jednostavnih aplikacija gdje je veličina poruka pretežito mala
- Efikasnost se temelji na modificirajućem blokovskom šifriranju koje izbjegava bilo kakvo inicijalno računanje
- fleksibilnost koja omogućuje korisniku proizvoljan odabir veličina ključa i modificirajućih podataka
- Otporan na side-channel napade
- Može se koristiti u Internetskom prometu kao i kod lightweight aplikacija gdje su veličine paketa koje se šalju dosta male



KETJE

- Algoritmi koji koriste niz operacija nazvan KECCAK- p permutacije
- Oslanjaju se na MonkeyDuplex konstrukciju koja održava stanje i ima broj rundi n_r
- Autentifikaciju poruka osigurava MonkeyWrap koji se zasniva na MonkeyDuplex konstrukciji te kao ulaz prima zaglavlje A i tijelo poruke B i vraća kriptiranu poruku C i oznaku T
- WRAP podržava sesije (enkripciju niza poruka) kod koje je oznaka T za svaku poruku autentična obzirom na cijeli niz poruka

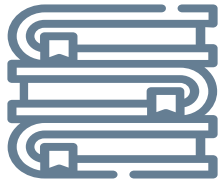


KETJE

- 4 autentične funkcije za enkripciju:
  - KETJE SR
  - KETJE JR
  - KETJE MINOR
  - KETJE MAJOR
- Maksimizacija kapaciteta nadoknađivanjem gubitka performanski smanjenjem rundi u KECCAK- p funkciji
- Zaštićen od side channel napada i u hardware- u i u software- u
- Primjena u uređajima s malim memorijskim resursima
- Sigurno slanje poruka korištenjem sigurnih čipova poput pametnih kartica

KEYAK

- Familija algoritama koja se zasniva na Motorist autentificirajućem enkripcijskom modulu i KECCAK- p permutacijskim funkcijama
- Svaki sloj Motorist modula zadužen je za osiguravanje različitih funkcionalnosti
    - Piston- koristi funkciju za permutacije te funkcije: Piston.Crypt za enkripciju ili dekripciju, Piston.Inject za ubacivanje meta podataka te Piston.GetTag koja dodaje poruci oznaku T
    - Engine- koristi 4 funkcije koje pozivaju funkcije Piston objekata: Engine.Spark, Engine.Wrap, Engine.InjectCollective te Engine.getTag
    - Motorist- kontrolira Engine objekte te poziva parametrizirane Piston objekte



KEYAK

- Postoji 5 instanci algoritma:

NAZIV	b	Broj paralelnih Piston objekata
River Keyak	800	1
Lake Keyak	1600	1
Sea Keyak	1600	2
Ocean Keyak	1600	4
Lunear Keyak	1600	8

- Preporuča se korištenje Lake Keyak instance
- Podupiru sesije u kojima cijeli niz poruka može biti autentificiran
- Sigurnost algoritma bazirana na tajnosti unutarnjih stanja Piston objekata čime se sprječavaju tzv. side channel napadi
- Omogućene su paralelna enkripcija ili dekripcija paralelnim korištenjem različitih Piston objekata

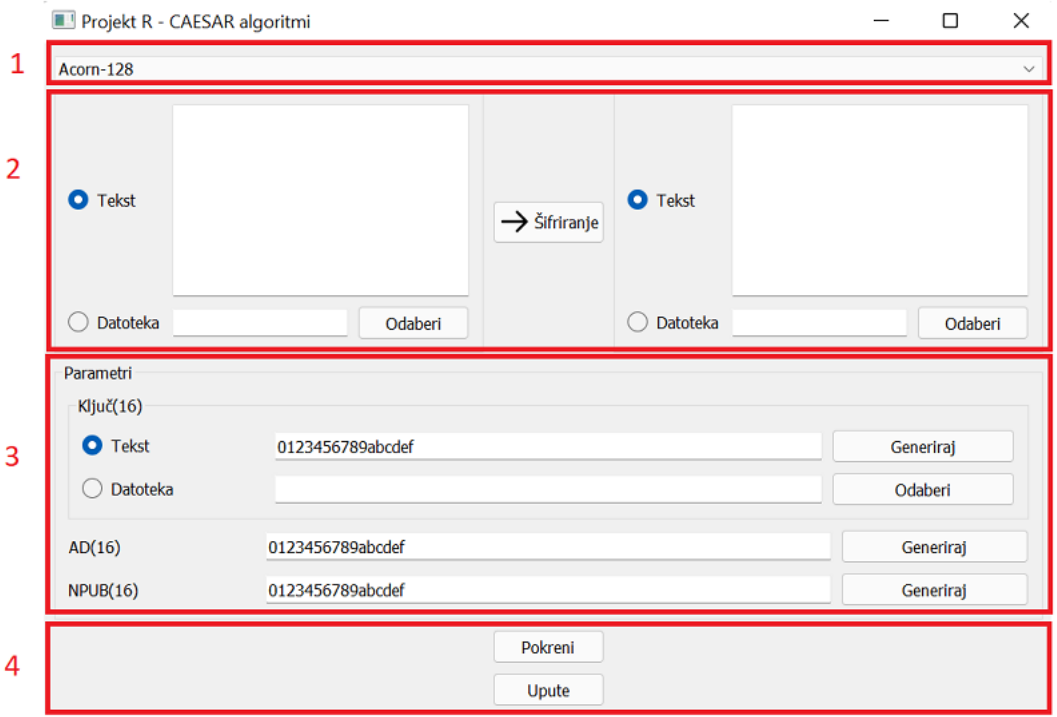
PROGRAMSKO RJEŠENJE

PROGRAM

- Programski jezik C++
- Moguća instalacija na Windows i Linux operacijskim sustavima
- Program omogućuje korisniku odabir algoritma kojim želi šifrirati određenu poruku ili datoteku
- Korisnik pomoću grafičkog sučelja odabire želi li šifrirati ili dešifrirati ulaznu poruku ili datoteku, algoritam šifriranja ili dešifriranja te bira želi li unijeti ručno parametre ili će iskoristiti defaultne

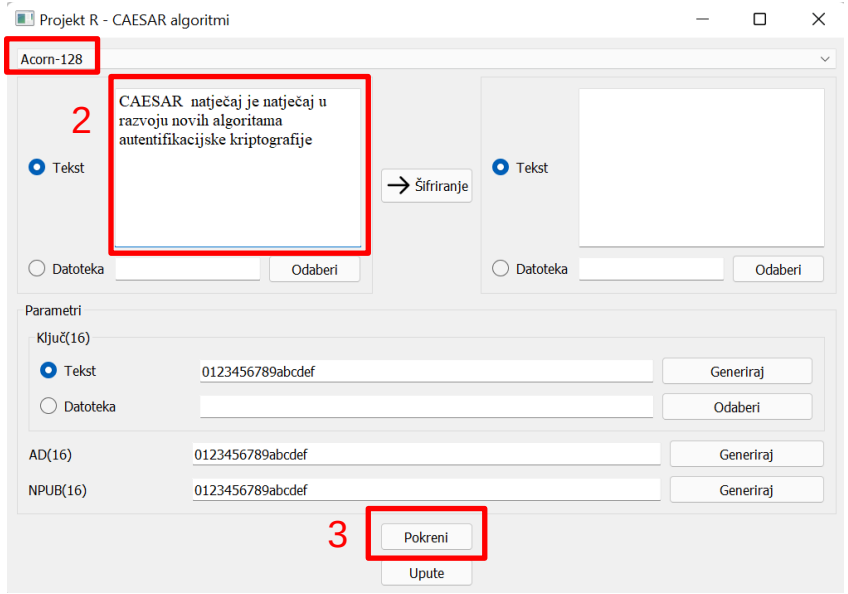
KORISNIČKO SUČELJE

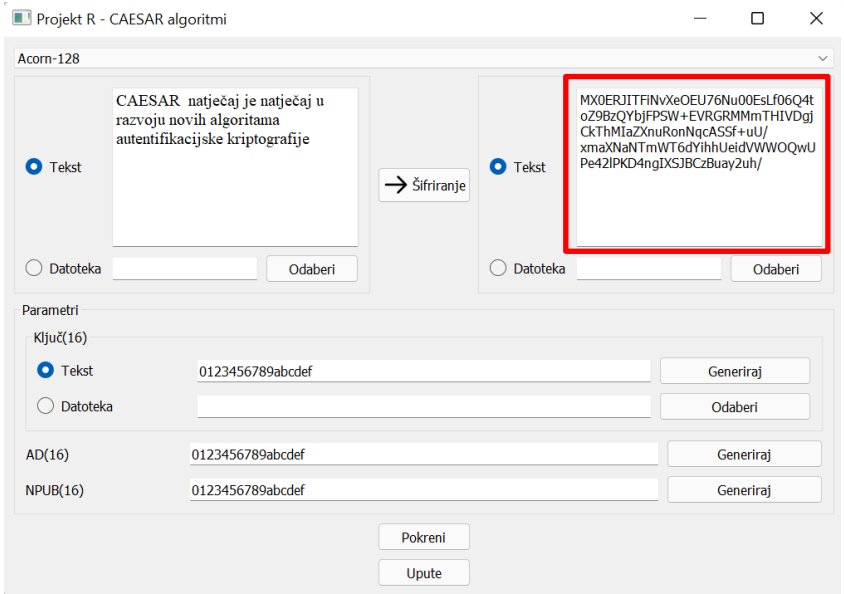
- Korisničko sučelje programske potpore se sastoji od 4 glavna dijela:



1. Dijela za odabir algoritma
2. Dijela za unos poruke te ispis izlaza algoritma
3. Dijela za unos parametara
4. Dijela za pokretanje algoritma te prikaza uputa za korištenje

PRIMJER KORIŠTENJA PROGRAMA (šifriranje teksta s pretpostavljenim parametrima):





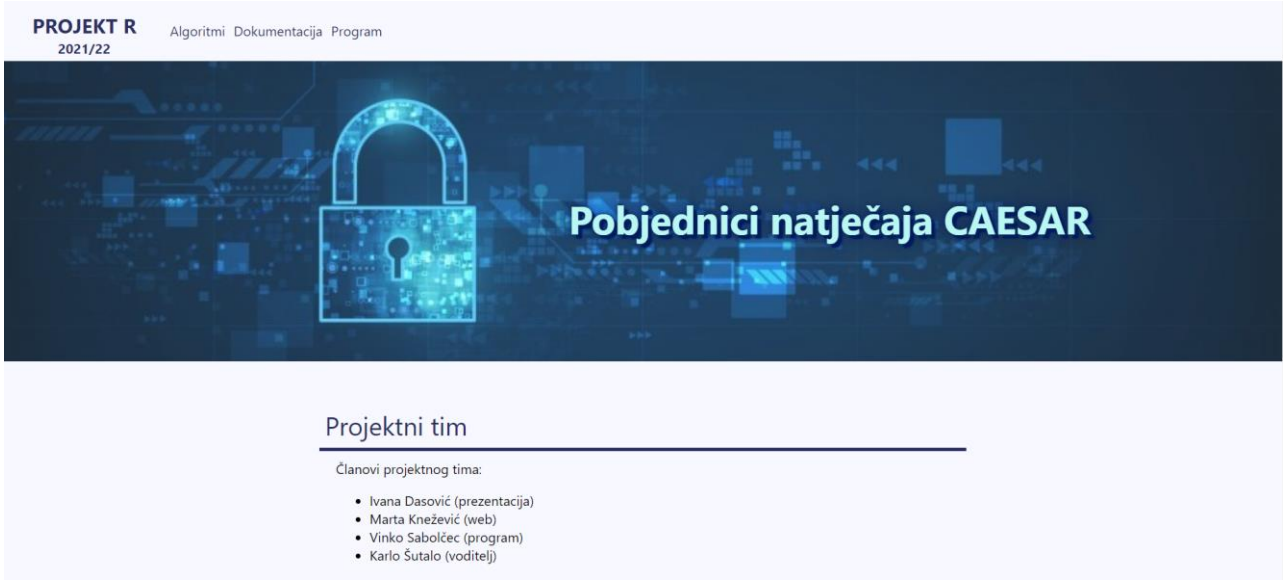
1. Odabir algoritma
2. Unos teksta koji se šifrira
3. Klik na gumb „Pokreni”

U označenoj kućici dobiva se šifrirani tekst

WEB STRANICA

WEB STRANICA

- Napravljena u edukativne svrhe
- Prikazuje kratak opis svih algoritama i omogućuje preuzimanje gotovog programskog rješenja, prezentacije i tehničke dokumentacije



PRIMJER WEB STRANICE

ASCON

Specifikacija algoritma

Algoritam ASCON pripada familiji ASCON_(a,b)-k-r algoritama za autentificiranu enkripciju.
Ulazni podaci za funkciju enkripcije su:

- Jasan tekst P - podijeljen u blokove podataka P_i duljine r bitova
- Asocirani podaci A - podijeljeni u blokove podataka A_i duljine r bitova