Implementacija OpenPGP protokola

PROJEKAT IZ ZAŠTITE PODATAKA

- školska 2021/2022. godina -

Autori:

Aleksandar Radošević 2018/0333

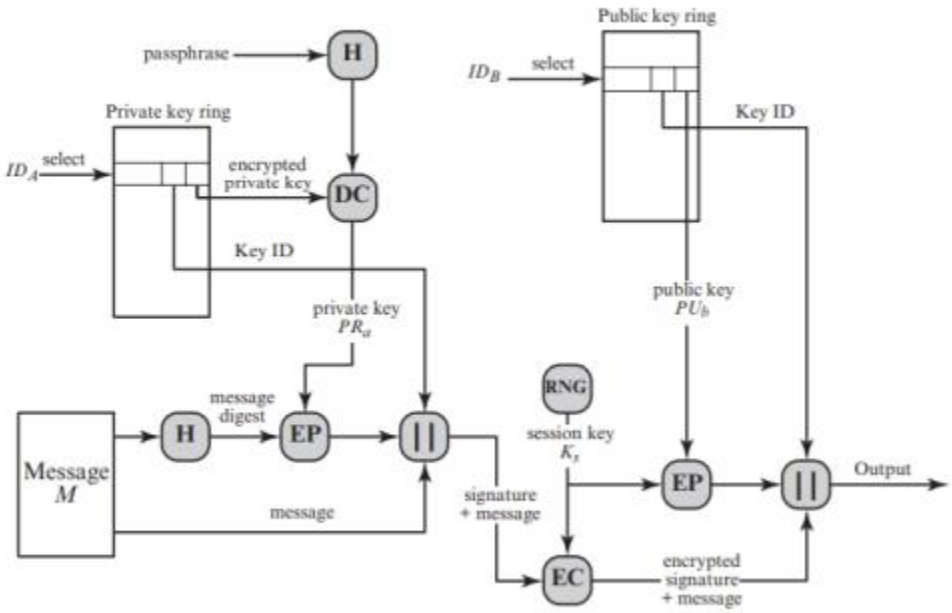
Luka Tomanović 2018/0410

U Beogradu, 01.06.2022. godine.

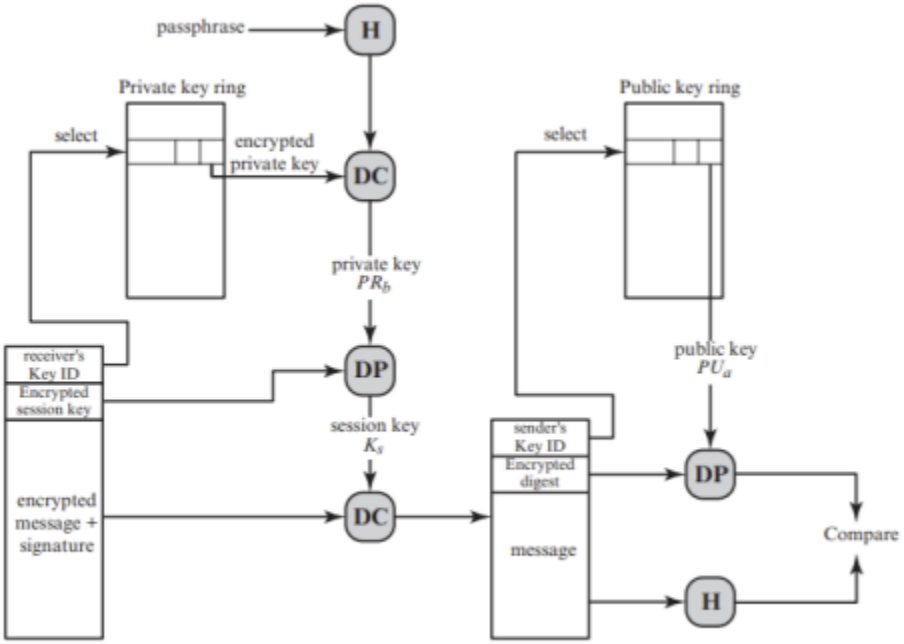
Sadržaj

Implementirani algoritmi u okviru projekta

Prikaz PGP šeme za slanje poruka:

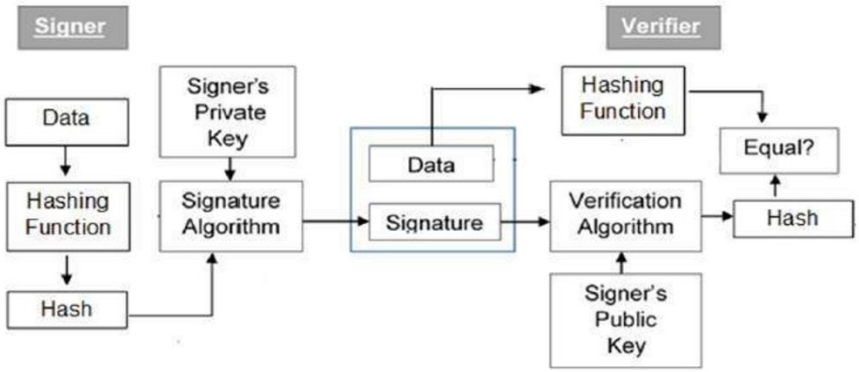


Prikaz PGP šeme za prijem poruka:



Algoritam za digitalno potpisivanje (DSA)

Digitaln potpis je važan element u digitalnom svetu komunikacije. Omogućava proveru identiteta autora neke poruke, kao i proveru autentičnosti sadržaja iste. Kako bi to obezbedio, digitalni potpis mora da zavisi od poruke koju potpisuje, mora da koristi informaciju jedinstvenu za autora, treba da bude lak za kreiranje, prepoznavanje i verifikaciju, a težak za falsifikovanje.



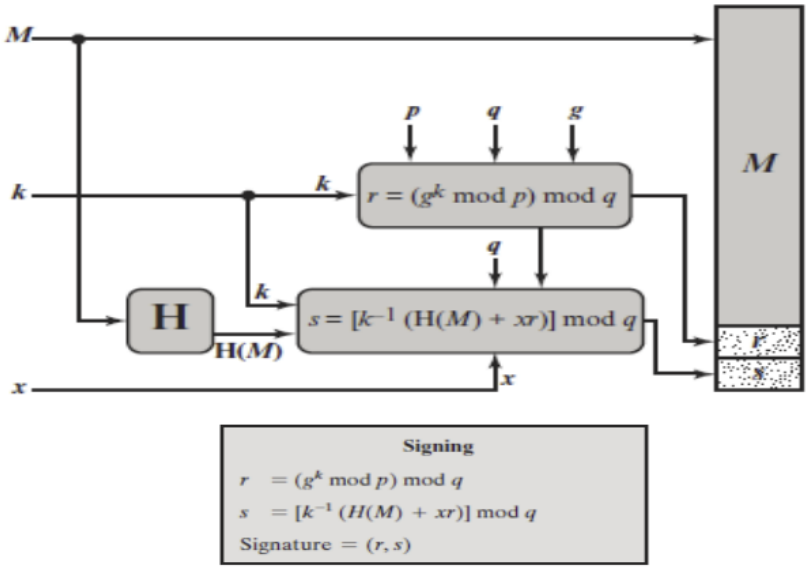
DSA (Digital Signature Algorithm)

DSA je algoritam za kreiranje digitalnih potpisa čija je matematička pozadina bazirana na modularnoj aritmetici i diskretnim logaritmima.

Koraci u DSA algoritmu:

1. Generisanje heša poruke
    a. Izračunati heš vrednost poruke koja se potpisuje
    (npr. heš poruke se može dobiti korišćenjem algoritama SHA, MD5...)
    U projektu je za DSA 1024 korišćen SHA-1 algoritam, a za DSA 2048 je korišćen SHA-256.
    Napomena: voditi računa o tome kolika je dužina generisanog heša zbog koraka 2.b. koji sledi.
    $\boldsymbol{H} - \ izračunati\ heš$; $|\boldsymbol{H}| - dužina\ generisanog\ heša$
2. Generisanje ključa
    a. Izabrati dužinu ključa **L** (512, 1024, 2048,...)
    b. Izabrati broj **N** takav da je $\boldsymbol{N} < \boldsymbol{L}$ i $\boldsymbol{N} \leq |\boldsymbol{H}|$
    Prema FIPS 186-4 specificirane vrednosti su (L,N): (1024, 160), (2048, 224), (2048, 256), or (3072, 256)
    FIPS – Federalni standard za obradu informacija
    c. Izabrati prost broj **q** dužine **N**
    d. Izabrati prost broj **p** dužine **L**, tako da važi $(p-1)\ mod\ q = 0$, odnosno q je prost delilac broja p-1
    e. Izabrati slučajan broj **h** iz skupa $\{2, \dots, p-2\}$
    f. Izračunati ceo broj g, tako da važi $g = h^{\frac{p-1}{q}} \bmod \mathrm{p}\ ;\ 1 < \mathrm{g} < \mathrm{p}$
    g. Izabrati slučajan broj x tako da važi $0 < \mathrm{x} < \mathrm{q}$
    h. Izračunati $y = g^x\ mod\ p$
    i. **Privatni** ključ čini uređena četvorka $\{\mathrm{p}, \mathrm{q}, \mathrm{g}, \mathbf{x}\}$
    j. **Javni** ključ čini uređena četvorka $\{\mathrm{p}, \mathrm{q}, \mathrm{g}, \mathbf{y}\}$

3. Generisanje potpisa
    a. Izabere se pseudoslučajan ceo broj **k** ($0 < \mathrm{k} < \mathrm{q}$), koji čini sesijski ključ
    b. Izračunamo $\boldsymbol{r} = \left(g^k \ mod \ p\right) \ mod \ q$. U slučaju da se dobije r = 0, potrebno je izabrati novo k (korak 3.a) i ponovo izračunati r.
    c. Izračunamo $\boldsymbol{s} = (k^{-1} * (H + x * r)) \ mod \ q$. U slučaju da se dobije s = 0, potrebno je izabrati novo k (korak 3.a) i vratiti se na korak 3.b.
    d. Potpis čini uređeni par $(\boldsymbol{r}, \boldsymbol{s})$



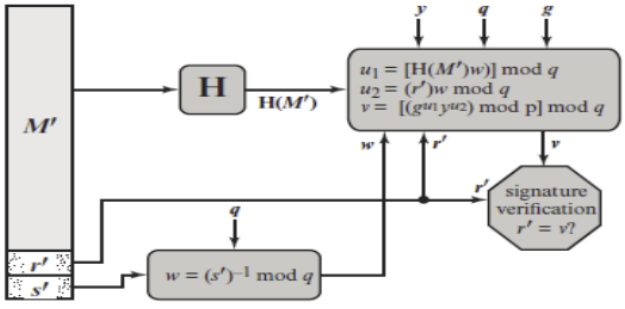
Signing

$r = (g^k \bmod p) \bmod q$

$s = [k^{-1}(H(M) + xr)] \bmod q$

Signature $= (r, s)$

4. Provera potpisa
    a. Proveriti da li važi za dobijene r i s (na slici označeni kao r` I s`): $0 < \mathrm{r} < \mathrm{q}$ i $0 < \mathrm{s} < \mathrm{q}$
    b. Izračunati $w = \ s^{-1} \ mod \ q$
    c. Izračunati $u1 = \ H * w \ mod \ q$
    d. Izračunati $u2 = \ r * w \ mod \ q$
    e. Izračunati $v = ((g^{u1} * y^{u2}) \ mod \ p) \ mod \ q$
    f. Ako važi $v = r$, potpis je validan.



Verifying

$w = (s')^{-1} \bmod q$

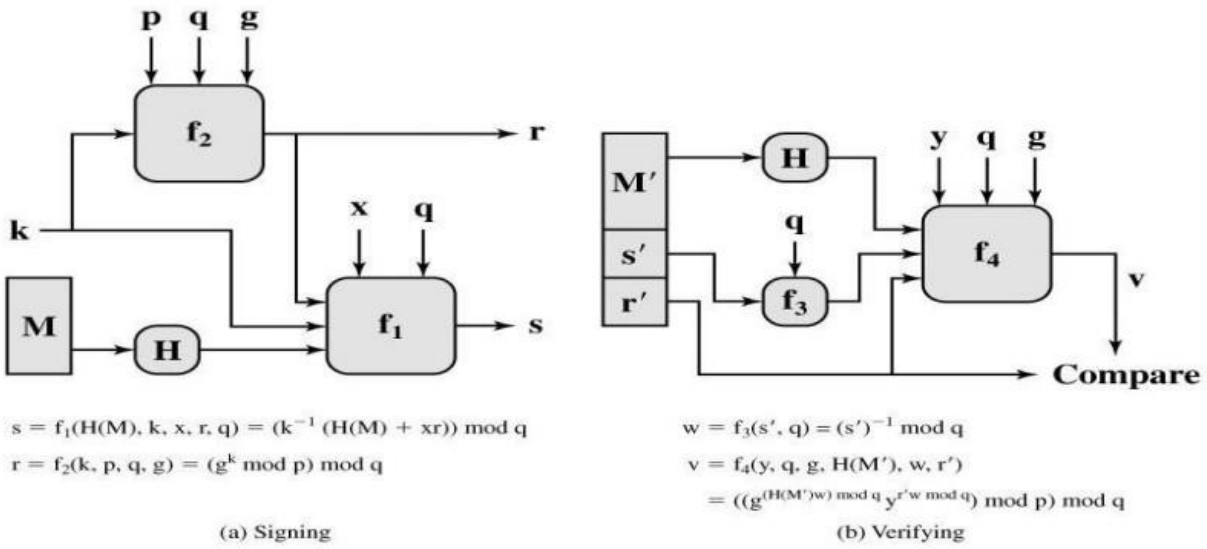
$u_1 = [H(M')w] \bmod q$

$u_2 = (r')w \bmod q$

$v = [(g^{u1}y^{u2}) \bmod p] \bmod q$

TEST: $v = r'$

Konačni pregled šeme DSA algoritma



Algoritmi za simetrično šifrovanje (AES)

Šifrovanje(enkripcija) je važan element u digitalnom svetu komunikacije jer obezbedjuje tajnost pri razmeni poruka.

U ovom projektu korišćeni su 3DES sa EDE strukturom i AES 128 kao algoritmi za simetrično šifrovanje.

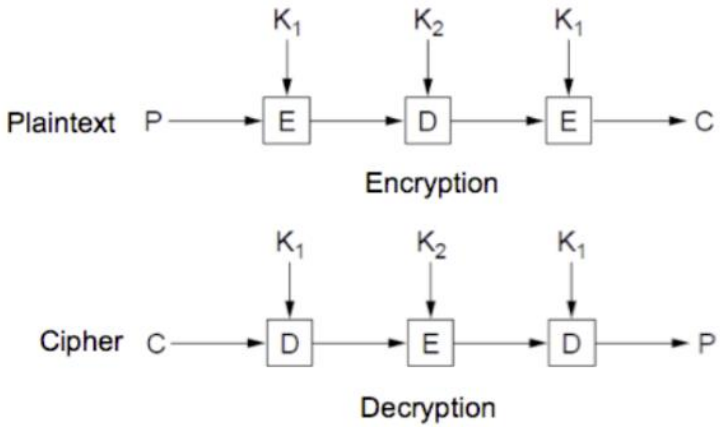
3DES(Triple Data Encryption Standard)

3DES je blokovski algoritam za simetrično šifrovanje.

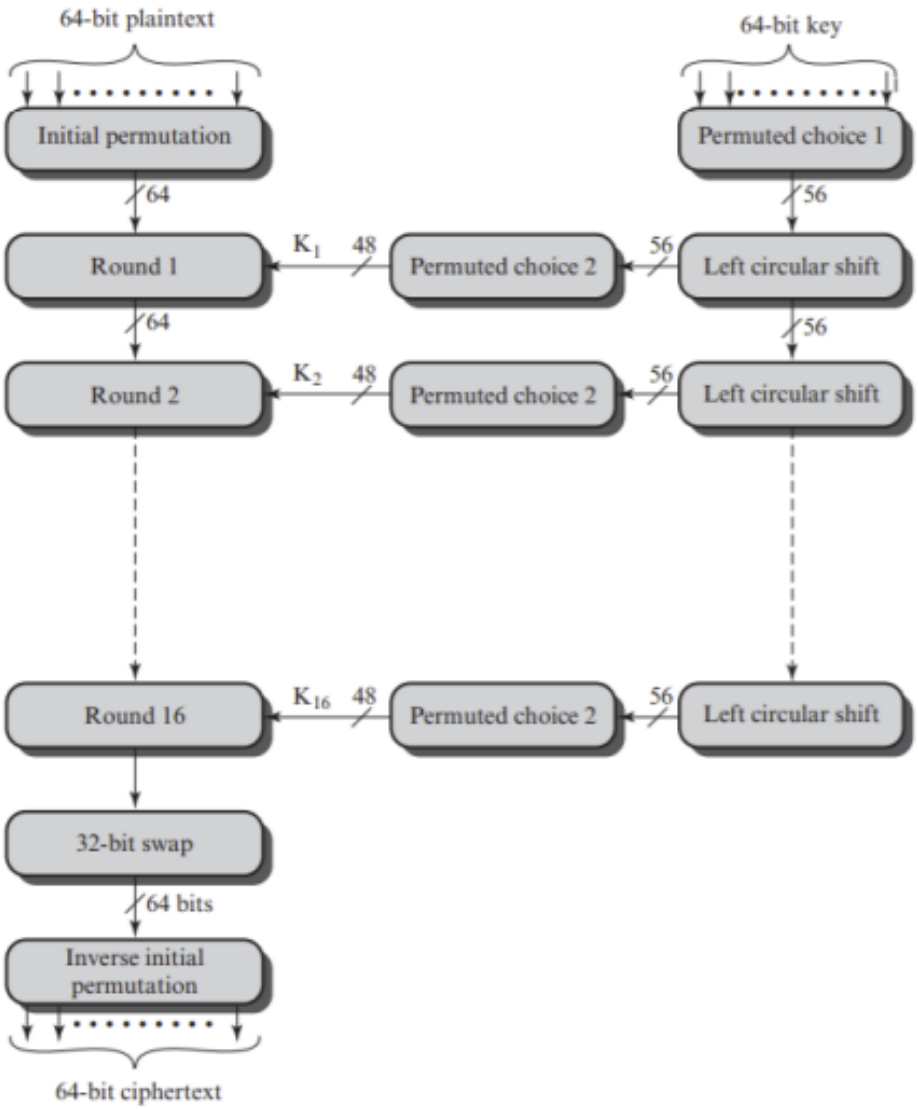
Kako bi se izbegao meet-in-the-middle 3DES je zamenio DES, svog prethodnika. 3DES je zapravo primena DES algotima tri puta za redom, tako da je većina osobina zadržana(blok veličine 64-bita, ključ veličine 56-bita), a sigurnost povećana.

Šifrovani tekst se dobija na sledeći način: $C = EK1\ [DK2\ [EK1\ [P]]]$. Kao što možemo videti dovoljna su nam dva različita ključa. Ako je K1 = K2 algoritam se svodi na običan DES algoritam, dok je u cilju povećane sigurnosti moguće koristiti i tri različita ključa.

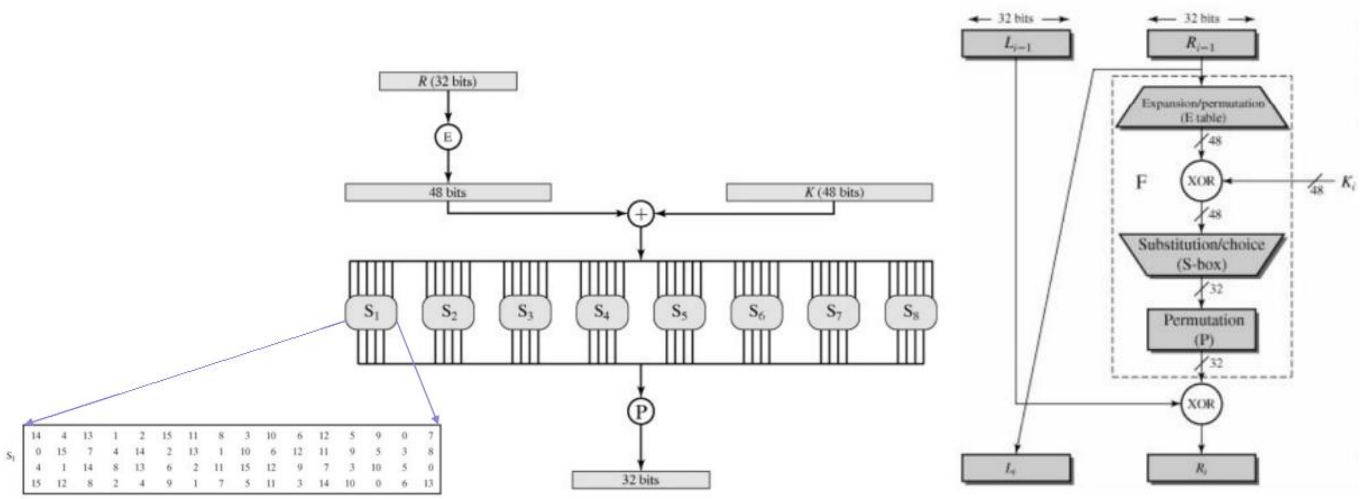
Pošto je u pitanju simetrični algoritam, necemo dodatno obradjivati dekripciju $D = DK1\ [EK2\ [DK1\ [P]]]$.



Prikaz DES algoritma koji se koristi u 3DES algoritmu



Prikaz jedne runde u DES algoritmu



AES (Advanced Encryption Standard)

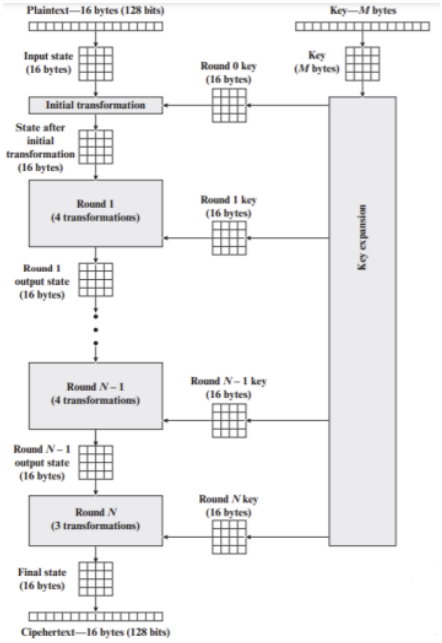
AES je blok algoritam namenjen da zameni DES u komercijalnim aplikacijama.

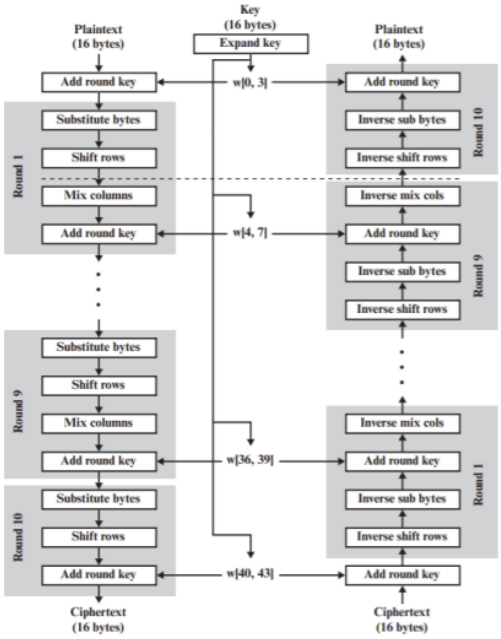
Koristi 128 bita za veličinu bloka i 128, 192 ili 256 bita za veličinu ključa.

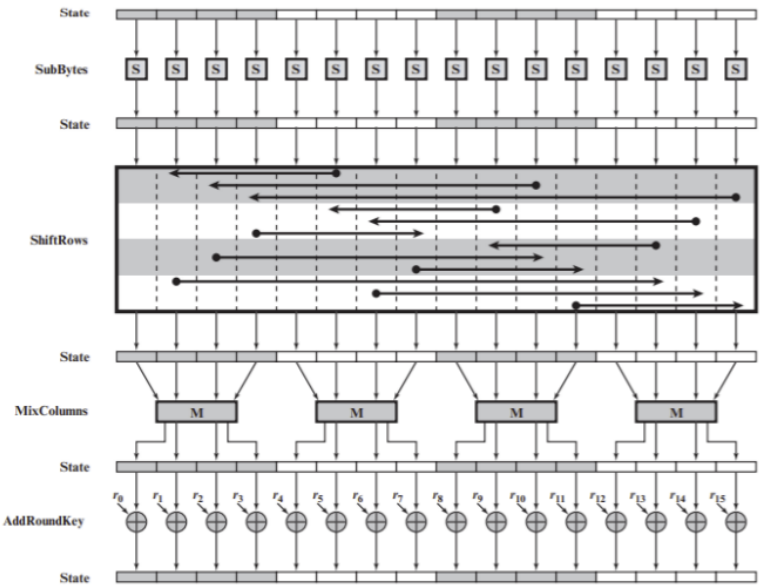
U projektu je korišćen AES algoritam sa dužinom ključa od 128 bita.

Veličina ključa (words/bytes/bits)	4/16/128	6/24/192	8/32/256
Veličina bloka (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Broj rundi	10	12	14
Veličina ključa iteracije (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Veličina ekspandovanog ključa (words/bytes)	44/176	52/208	60/240

Prikaz rada algoritama dat je na sledecim slikama:







Algoritam za šifrovanje sesijskog ključa(ElGamal)

U realizaciji ovog projekta korišćen je ElGamal kako bi se zaštitila tajnost sesijskog ključa koji se koristi za simetričnu enkripciju.

ElGamal je algoritam za asimetrično šifrovanje u kriptografiji sa javnim ključem i zasniva se na Diffie-Hellman algoritmu.

U daljim koracima sesijski ključ koji je potrebno zaštiti smatraćemo porukom **M**.

Koraci u ElGamal algoritmu:

1. Generisanje ključeva
    a. Izabrati prost broj **q** i njegov primitivni koren $\boldsymbol{\alpha}$.
    b. Generisati slučajan broj $\mathbf{X_a}$, tako da važi $1 < X_a < q - 1$. $\mathbf{X_a}$ predstavlja **privatni** ključ.
    c. Izračunati $\boldsymbol{Y_a} = \alpha^{X_a} \, mod \, q$. $\mathbf{Y_a}$ predstavlja **javni** ključ zajedno sa $q \; i \; \alpha$.
2. Šifrovanje poruke
    a. Odrediti cikličnu grupu **G** reda q, sa generatorom α. $G = \{ e, \alpha^1, \alpha^2, \alpha^3, \ldots, \alpha^q \}$
    Napomena: na dalje nećemo naglašavati da je potrebno sve operacije raditi po modulu q.
    b. Mapirati poruku M u element **m** koji pripada G koristeći reverzibilne funkcije mapiranja
    c. Izabrati slučajan broj K iz skupa $\{1, \ldots \, , \mathrm{q} - 1\}$
    d. Izračunati $s = {Y_a}^K$, takozvanu deljenu tajnu.
    e. Izračunati $c1 = \alpha^K$
    f. Izračunati $c2 = m * s$
    g. Šifrovanu poruku čini uređeni par $(c1, c2)$.
3. Dešifrovanje poruke
    a. Izračunati $\boldsymbol{s} = c1^{X_a} = \alpha^{K * X_a} = {Y_a}^K$.
    b. Izračunati s^{-1}, multiplikativni inverz od s u grupi G.
    c. Izračunati $m = c2 * s^{-1} = m * s * s^{-1}$
    d. Mapirati m nazad u originalni tekst poruke M.