(19) REPUBLIKA HRVATSKA
DRŽAVNI ZAVOD ZA
INTELEKTUALNO VLASNIŠTVO

(21) Broj prijave: HR P20020179A A2

HR P20020179A A2

(12) PRIJAVA PATENTA

(51) Int. Cl.[7]: **H 04 L 9/00**

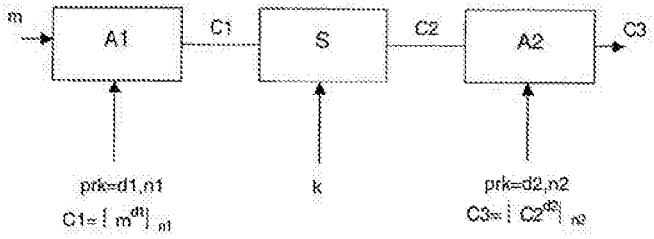
(22) Datum podnošenja prijave patenta u HR: 27.02.2002.
(43) Datum objave prijave patenta u HR: 29.02.2004.
(86) Broj međunarodne prijave: PCT/IB00/01157
Datum podnošenja međunarodne prijave 24.08.2000.
(87) Broj međunarodne objave: WO 01/17159
Datum međunarodne objave 08.03.2001.

(31) Broj prve prijave: 1573/99
60/194,171
(32) Datum podnošenja prve prijave: 30.08.1999.
03.04.2000.
(33) Država ili organizacija podnošenja prve prijave: CH
US

(71) Podnositelj prijave: **Nagracard SA, 22, route de Genève, 1033 Cheseaux-Sur-Lausanne, CH**
(72) Izumitelji: **Marco Sasselli, 20, chemin des Roches, 1803 Chardonne, CH**
Christophe Nicolas, 29, rue de Lausanne, 1028 Preverenges, CH
Michael John Hill, 10, route de Commugny, 1296 Coppet, CH
(74) Punomoćnik: CPZ - CENTAR ZA PATENTE d.d., ZAGREB, HR

(54) Naziv izuma: **VIŠEMODULNI POSTUPAK KODIRANJA**

(57) Sažetak: Kada se koristi modul za kodiranje/dekodiranje, postoje postupci za određivanje ključa ili ključeva koje koristi modul i to putem analize podataka koji ulaze ili izlaze iz modula. U svrhu uklanjanja tog nedostatka, predloženi višemodulni postupak uključuje modul koji započinje svoje operacije kodiranja/dekodiranja čim dobije na raspolaganje dio rezultata iz modula prije njega (gledano u smjeru toka podataka).



HR P20020179A A2

OPIS IZUMA

Predmetni izum se odnosi na područje kodiranja, ili šifriranja, te na dekodiranje ili dešifriranje podataka, a posebno podataka koji trebaju ostati nedostupni neovlaštenim osobama ili uređajima unutar sustava televizije uz plaćanje. U takvim sustavima, podaci se kodiraju u sigurnom okružju koje je opremljeno znatnom računalnom snagom, te se naziva podsustav za kodiranje. Zatim se podaci šalju, poznatim načinima, u najmanje jedan decentralizirani podsustav gdje se dekodiraju, uglavnom putem IRD uređaja (Integrated Receiver Decoder - integrirani prijemnik dekoder) i pomoću čip kratice. Moguće je da i neovlaštena osoba ostvari neograničeni pristup toj čip-kartici i decentraliziranom podsustavu koji radi s njom.

U praksi je poznato lančano povezivanje raznih načina kodiranja/dekodiranja u jedan sustav za kodiranje/dekodiranje. U cijelom tekstu koji slijedi, izraz kodiranje/dekodiranje će se koristiti za posebne načine kodiranja koji se koriste u većim sustavima za kodiranje/dekodiranje.

Dugo vremena se razmišljalo o optimiziranju rada tih sustava i to iz tri razloga, odnosno obzirom na brzinu, zauzet prostor memorije i sigurnost. Pod brzinom se razumijeva vrijeme potrebno za dekodiranje primljenih podataka.

Poznati su sustavi za kodiranje/dekodiranje sa simetričnim ključevima. Njihova sigurnost se može mjeriti kao funkcija nekoliko kriterija.

Prvi kriterij je onaj fizičke sigurnosti, koji se odnosi na lakoću ili poteškoće postupka istraživanja izdvajanjem određenih komponenti, na što se nadovezuje mogućnost njihove zamjene drugim komponentama. Te zamjenske komponente, čija je namjena da daju informaciju neovlaštenoj osobi o prirodi i načinu rada sustava za kodiranje/dekodiranje, ta osoba bira na taj način da ih ne otkrije, ili da budu što teže za otkrivanje, od strane ostatka sustava.

Drugi kriterij je kriterij sigurnosti sustava, a koji se odnosi na neovlaštene upade koji nisu u okvirima fizičkih upada već zahtijevaju analizu matematičkog tipa. Uobičajeno, te upade će vršiti snažna računala koja će pokušati razbiti algoritme i kodove šifriranja.

Načini kodiranja/dekodiranja sa simetričnim ključevima (lozinkama) su na primjer sustavi poznati kao DES (Data Encryption Standard - Standard za kodiranje podataka). Ti relativno stari načini sada nude samo sigurnost sustava i fizičku sigurnost koje su sasvim relativne. Naročito iz tog razloga se DES, čije su lozinke premale da zadovolje uvjete sigurnosti sustava, sve više zamjenjuje novim načinima kodiranja/dekodiranja ili s dužim lozinkama. Uglavnom, ti načini sa simetričnim ključevima zahtijevaju algoritme koji uključuju kružno kodiranje.

Ostale strategije upada (probijanja kodne zaštite) su poznate kao Jednostavna analiza napajanja (Simple Power Analysis) i Vremenska analiza. Kod Jednostavne analize napajanja, koristi se činjenica da je mikroprocesor čiji je zadatak šifriranje ili dešifriranje podataka spojen na izvor napona (uglavnom 5 volti). Kada je (mikroprocesor) u stanju mirovanja, kroz njega prolazi struja jačine i. Kada je aktivan, stalna jačina / je ovisna ne samo o ulaznim podacima, već i o algoritmu dekodiranja. Jednostavna analiza napajanja se sastoji u mjerenju struje / kao funkcije vremena. Iz toga se može izvesti dedukcijom algoritam koji mikroprocesor izvodi.

Na isti način, postupak Vremenske analize se sastoji u mjerenju trajanja računanja kao funkcije uzorka prikazanog modulu za dekodiranje. Dakle, odnos između prikazanog uzorka i vremena za računanje rezultata omogućava da se otkriju tajni parametri modula za dekodiranje kao što je lozinka. Takav sustav je opisan u dokumentu "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and other Systems" kojeg je objavio Paul Kocher, Cryptography Research, 870 Market St, Suite 1088, San Francisko, CA-USA.

Za poboljšanje sigurnosti sustava šifriranja, predlagani su algoritmi s asimetričnim lozinkama, poput tzv. RSA (Rivest, Shamir i Adleman) sustava. Ti sustavi uključuju formiranje dviju lozinki koje međusobno odgovaraju, jedne tzv. javne lozinke koja služi kod šifriranja, te druge tzv. privatne lozinke koja se koristi za dešifriranje. Ti algoritmi osiguravaju visoku razinu sigurnosti, kako sustava tako i fizičke sigurnosti. Oni su s druge strane sporiji od tradicionalnih sustava, posebno u fazi kodiranja.

Najnoviji postupci probijanja sustava zahtijevaju takozvani DPA koncept, što je kratica za Differential Power Analysis (diferencijalna analiza snage). Ti postupci se temelje na pretpostavkama, koje je moguće potvrditi nakon velikog broja pokušaja, o postojanju znamenke 0 ili 1 na danom mjestu ključa za kodiranje. Oni skoro da nisu destruktivni, zbog čega ih se uglavnom teško otkriva, te zahtijevaju kako komponentu za fizički upad tako i komponentu za matematičku analizu. Način njihovog rada podsjeća na postupke za istraživanje naftnih polja, kod kojih se eksplozija poznate snage uzrokuje na površini i pri kojima slušalice i sonde, postavljene na sličnim i poznatim udaljenostima od mjesta eksplozije, omogućavaju izvođenje pretpostavki o stratigrafskom sastavu slojeva ispod površine bez nužnosti

provođenja opsežnih iskopavanja, koristeći efekt refleksije udarnih valova od granica sedimentarnih slojeva ispod površine. DPA upadi su posebno opisani u § 2.1. dokumenta "A Cautionary Note Regarding Evaluation of AES Candidates on Smart-Cards", kojeg su 1. veljače 1999 izdali Suresh Chari, Charanjit Jutla, Josvula R. Rao i Pankaj Rohatgi, sa IBM TJ. Watson Research Center, Yorktown Heights, NY.

Potreba suprotstavljanja DPA upadima nužno zahtijeva primjenu tzv. sustava za blokiranje (zagušenje) s "bijeljenjem", ili u ulaznoj informaciji, ili na izlazu algoritma za šifriranje/dešifriranje. Postupak bjeljenja je opisan u § 3.5 istog prije navedenog dokumenta.

Osim toga, činjenica da su računalne snage ograničene u decentraliziranom podsustavu televizijskog sustava s plaćanjem izaziva problem, koji nikad do sada nije bio uspješno riješen, za izvođenje ulančavanja koje je prije dovoljno opisano.

Cilj predmetnog izuma je da omogući postupak šifriranja/dešifriranja koji je otporan na moderne postupke istraživanja poput prethodno opisanih.

Željeni cilj predmetnog izuma je postignut postupkom opisanim u dijelu kojim su naznačene karakteristike Patentnog zahtjeva 1.

Posebna karakteristika ovog postupka je u činjenici da među-modul ne započinje s radom kada je rezultat iz prethodnog modula (modula koji se nalazi prije njega u smjeru protoka informacija) dovršen, već započinje odmah čim mu je stavljen na raspolaganje barem dio informacije. Na taj način, za vanjskog promatrača, nije moguće ustanoviti ulazne ili izlazne uvjete za taj modul.

Obzirom da se dešifriranje događa u decentraliziranom podsustavu koji radi povezano s čip-karticom, pri čemu ta čip-kartica raspolaže samo s relativno ograničenom snagom računanja u usporedbi s pod-sustavom za dešifriranje, povoljno je na primjer koristiti javni asimetrični ključ, koji radi relativno brzo, za vrijeme zadnjih koraka dešifriranja. To omogućava s jedne strane da se zaštiti nepovredivost sustava kod izlaska iz postupka, a s druge strane da se koncentrira računalna snaga, u osnovi vezano na šifriranje pomoću privatne šifre, u podsustavu za šifriranje.

Otkriveno je da je dodatna sigurnost omogućena povezivanjem, ili djelomičnim umetanjem, dvaju načina kodiranja/dekodiranja koji slijede jedan iza drugog. Treba razumjeti da to povezivanje ili djelomično umetanje znači postupak koji se sastoji u započinjanju drugog načina kodiranja/dekodiranja podataka u trenutku kada prvi način kodiranja/dekodiranja podataka još nije završio svoj rad na istim podacima. To omogućava da se prikriju podaci u obliku u kojem bi se dobili radom prvog modula, a prije nego su podvrgnuti djelovanju drugog modula.

Ulančavanje može započeti čim su podaci koji su obrađeni na izlazu prvog modula na raspolaganju za obradu drugim modulom.

Ovaj izum omogućava zaštitu od prije navedenih upada kombiniranjem različitih načina kodiranja/dekodiranja u sustavu za šifriranje/dešifriranje, te po mogućnosti dopunjavanje sigurnosti povezivanjem ili djelomičnim umetanjem određenim redoslijedom, pri čemu ti načini slijede jedan iza drugoga.

U posebnoj izvedbi ovog izuma, sustav za šifriranje/dešifriranje uključuje jedan podsustav za kodiranje u kojem se jedan za drugim koriste tri algoritma:

a) asimetrični algoritam A1 s privatnom šifrom (ključem) d1. Taj algoritam A1 izvodi označavanje na nešifriranim podacima, predstavljenim porukom *m,* pri čemu ta operacija rezultira prvim kriptogramom *c1,* korištenjem matematičkih operacija koje su u profesiji uglavnom označene formulom: c1=m eksponent d1, modulo n1. U toj formuli *n1* tvori dio javnog ključa asimetričnog algoritma A1, modulo predstavlja dobro poznati matematički operator sukladnosti unutar skupa relativnih cijelih brojeva, a *d1* je privatni ključ algoritma A.
b) simetrični algoritam S koji koristi tajni ključ K. Taj algoritam pretvara kriptogram *c1* u kriptogram *c2.*
c) asimetrični algoritam A2 s privatnim ključem *d2* Taj algoritam A2 pretvara kriptogram *c2* u kriptogram *c3,* korištenjem matematičkih operacija, kako je prije navedeno: c3=c2 eksponent d2, modulo n2, u kojoj formuli *n2* tvori dio javnog ključa asimetričnog algoritma A2.

c1=m eksponent d1, modulo n1. U toj formuli *n1* tvori dio javnog ključa asimetričnog algoritma A2.

Kriptogram c3 napušta podsustav za šifriranje i dolazi u decentralizirani podsustav na već poznati način. U slučaju sustava televizije uz plaćanje, to može podjednako uključivati video podatke ili poruke.

Decentralizirani podsustav koristi, redoslijedom obrnutim od prije navedenog, tri algoritma A1', S' i A2'. Ta tri algoritma tvore dio tri načina za šifriranje/dešifriranje A1-A1', S-S' i A2-A2', raspodijeljeno između podsustava za kodiranje i decentraliziranog sustava, te predstavljaju sustav za kodiranje/dekodiranje.

a) algoritam A2' izvodi matematičku operaciju nad c3 kojom se ponovno dobiva c2 i označava se: c2=c3 eksponent e2, modulo n2. U toj formuli, skup koji se sastoji od e2 i n2 je javni ključ asimetričnog algoritma A2-A2'.
b) simetrični algoritam S' koji koristi tajni ključ K ponovno uspostavlja kriptogram *c1*.
c) asimetrični algoritam A1' s javnim ključem *e1,* n1 ponovno uspostavlja *m* izvođenjem matematičke operacije označene: m=c1 eksponent e1 mod n1.

Dopunjavanje, u decentraliziranom sustavu, se sastoji u započinjanju koraka dekodiranja e) dok c2 još nije u cijelosti ponovno uspostavljen prethodnik korakom d), te u započinjanju koraka dekodiranja f) doko c1 još nije u cijelosti ponovno dobiven korakom e. Prednost je u osujećivanju upada koji, na primjer, ima prvenstveno cilj ekstrahiranja, unutar decentraliziranog podsustava, kriptograma *c1* na kraju koraka e, kako bi ga se usporedilo s nešifriranim podacima *m,* a zatim pomoću *c1* da izvrši upad u algoritam A1', te postepeno unatrag da pronađe lanac kodiranja.

Dopunjavanje nije nužno u podsustavu kodiranja koji je instaliran u sigurnom fizičkom okružju. S druge strane ono je korisno u decentraliziranom podsustavu. U slučaju televizije uz plaćanje, IRD je u stvari instaliran u prostorijama pretplatnika i može biti predmet upada prije opisanog tipa.

Treba shvatiti da pokušaj upada u kombinaciju od tri dopunjena algoritma za kodiranje A1', S', i A2' ima puno manje šanse za uspjeh nego u slučaju da su kriptohrami c1 i c2 u potpunosti rekonstruirani između svakog koraka d), e) i f). Osim toga, iz činjenice da se algoritmi A1' i A2' koriste s javnim ključevima e1, n1 i e2, n2 proizlazi da je jako smanjena potreba za elementima računalne obrade u decentraliziranom podsustavu u odnosu na one u podsustavu za kodiranjc.

Kao primjer te da se utvrde činjenice, treba navesti da su koraci a) i c), što znači koraci šifriranja pomoću privatnih ključeva, su 20 puta duži od koraka dešifriranja d) i f) s javnim ključevima.

U posebnoj izvedbi predmetnog izuma, izvedenoj iz prethodne, algoritmi A1 i A2 su identični njihovim protudijelovima A1' i A2'.

U drugoj posebnoj izvedbi ovog izuma, također izvedenoj iz prethodne, u koraku c) se koristi javni ključ e2, n2 asimetričnog algoritma A2, dok se u koraku d) kriptogram c3 dešifrira pomoću privatnog ključa d2 tog algoritma. Ova izvedba predstavlja moguću alternativu kada su mogućnosti elemenata decentraliziranog podsistema u smislu računalne snage daleko od onih koje se može postići.

Iako se čip-kartice koriste pretežno za dešifriranje podataka, postoje također čip-kartice koje posjeduju karakteristike potrebne za izvođenje operacija šifriranja. U tom slučaju, prije opisani načini upada se odnose i na te kartice za šifriranje koje rade, odnosno koriste se, izvan zaštićenih lokacija kao što je upravljački centar. Iz tog razloga se postupak u skladu s predmetnim izumom primjenjuje također i na serijske operacije šifriranja, što znači da slijedeći modul (u smjeru strujanja podataka) započinje svoju operaciju šifriranja čim dobije dio informacija koje je isporučio modul prije njega. Taj postupak ima prednost mogućnosti umetanja različitih modula za šifriranje, a posljedica toga je ta, da rezultat iz prethodnog (u smjeru strujanja podataka) modula nije u cijelosti dostupan u određenom trenutku. Osim toga, slijedeći modul nc započinjc svojc opcracijc s potpunim rczultatom vcć na dijclovima, čimc sc onemogućava tumačcnjc načina rada modula u odnosu na poznato ulazno ili izlazno stanje.

Predmetni izum će biti bolje shvaćen pomoću priloženih crteža, danih samo kao neograničavajući primjer, na kojima:
Slika 1 predstavlja operacije šifriranja
Slika 2 predstavlja operacije dešifriranja
Slika 3 predstavlja alternativni postupak šifriranja.

Na slici 1, skup podataka m se uvodi u lanac šifriranja. Prvi element A1 izvodi operaciju šifriranja korištenjem tzv. privatnog ključa, koji uključuje eksponent d1 i modulo n1. Rezultat te operacije je predstavljen sa C1, U skladu s načinom rada predmetnog izuma, čim je dio rezultata C1 raspoloživ, slijedeći modul započinje svoj rad. Taj slijedeći modul S izvodi njegovu operaciju šifriranja pomoću tajnog ključa. Odmah nakon što je djelomično raspoloživ, rezultat C2 se prenosi u modul A2 za treću operaciju šifriranja korištenjem tzv. privatnog ključa koji sadrži eksponent d2 i modulo n2. Konačni rezultat, ovdje označen C3, je spreman za prijenos poznatim načinima poput zračnih valova ili kabelom.

Slika 2 prikazuje sustav kodiranja koji je sastavljen od tri modula za dekodiranje A1', S', A2' koji su slični onima koji služe za kodiranje, ali su postavljeni obrnutim redoslijedom. Dakle, prvo se započinje s modulom A2' koji izvodi njegovu operaciju kodiranja na temelju tzv. javnog ključa kojeg čini eksponent e2 i modulo n2. Na isti način kao za kodiranje, čim je dio rezultata C2 iz modula A2' raspoloživ, on se prenosi u modul S' za drugu operaciju dekodiranja. Za završetak dekodiranja, modul A1' izvodi njegovu operaciju na temelju tzv. javnog ključa kojeg čini eksponent e1 i modulo n1.

U posebnoj izvedbi predmetnog izuma, ključevi dvaju modula A1 i A2 su identični, što znači da je na strani kodiranja, d1=d2 i n1=n2. Analogno, za vrijeme dekodiranja, e1=e2 i n1=n2. U ovom slučaju, riječ je o privatnom ključu d, n i o javnom ključu e, n.

U drugoj izvedbi, kako je prikazano na slikama 3 i 4, modul A2 koristi tzv. javni ključ umjesto tzv. privatnog ključa. U trenutku kodiranja, javni ključ e2, n2 koristi modul A2, (vidi Sl. 3), a za vrijeme dekodiranja (vidi Sl. 4), modul A2' koristi za rad privatni ključ d2, n2. Iako ova konfiguracija izvodi rad prekomjeran za set za kodiranje, korištenje privatnog ključa povećava sigurnost koju nudi modul A2.

Primjer ilustriran na Slikama 3 i 4 nije ograničavajući u odnosu na druge kombinacije. Na primjer, moguće je konfigurirati modul A1 tako, da izvodi operaciju kodiranja s javnim ključem, a dekodiranje s privatnim ključem.

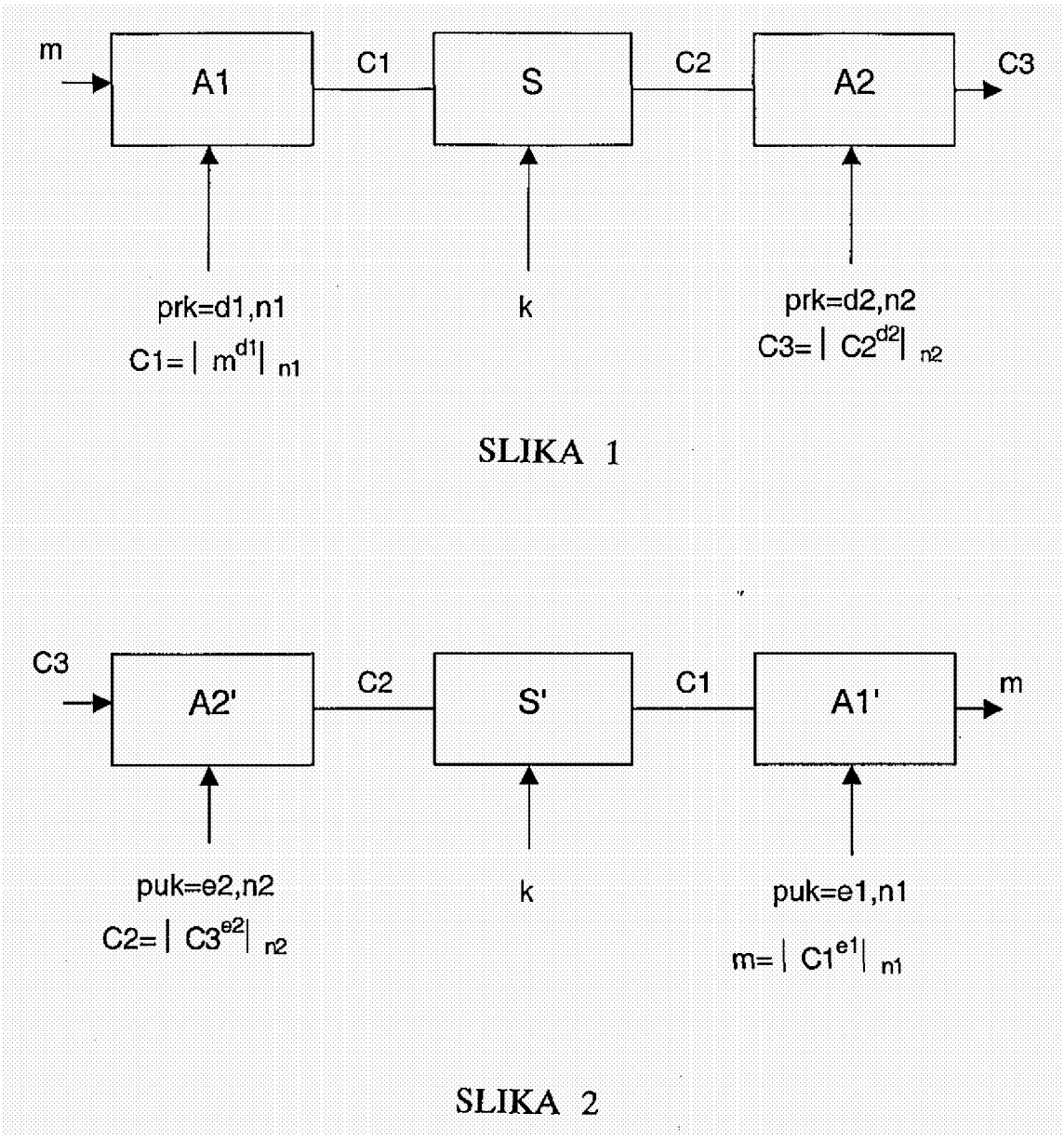
Također je moguće zamijeniti modul za kodiranje/dekodiranje koji ima tajni ključ S s tipom modula s asimetričnim ključevima istog tipa kao moduli A1 i A2.

PATENTNI ZAHTJEVI

1. Sustav za kodiranje i dekodiranje koji koristi nekoliko modula za kodiranje/dekodiranje spojenih u seriju, **naznačen time**, da slijedeći (u smjeru strujanja podataka) modul za kodiranje/dekodiranje započinje svoj rad čim mu je na raspolaganju dio rezultata iz modula za kodiranje/dekodiranje prije njega.
2. Postupak u skladu s Patentnim zahtjevom 1, **naznačen time**, da slijedeći (u smjeru strujanja podataka) modul za dekodiranje započinje svoju operaciju čim mu je na raspolaganju dio rezultata iz modula prije njega.
3. Postupak u skladu s Patentnim zahtjevom 1, **naznačen time**, da slijedeći (u smjeru strujanja podataka) modul za kodiranje započinje svoju operaciju čim mu je na raspolaganju dio rezultata iz modula prije njega.
4. Postupak u skladu s Patentnim zahtjevima 1 do 3, **naznačen time**, da uključuje tri modula (A1, S, A2), pri čemu je središnji modul (S) tipa s tajnim simetričnim ključem (k).
5. Postupak u skladu s prethodnim patentnim zahtjevom, **naznačen time**, da su prvi modul (A1) i zadnji modul (A2) u slučaju kodiranja, te prvi modul (A2) i zadnji modul (A1) u slučaju dekodiranja RSA tipa s asimetričnim ključevima, tj. s privatnim i javnim ključem.
6. Postupak u skladu s prethodnim patentnim zahtjevom, **naznačen time**, da dva modula (A1, A2) koriste tzv. privatni ključ (d, n; d1, n1; d2, n2) za kodiranje, a tzv. javni ključ (e, n; e1, n1; e2, n2) za dekodiranje.
7. Postupak u skladu s prethodnim patentnim zahtjevom, **naznačen time**, da dva modula (A1, A2) koriste isti skup privatnih ključeva (d, n) i javnih ključeva (e, n).
8. Postupak u skladu s Patentnim zahtjevom 6, **naznačen time**, da dva modula (A1, A2) koriste različiti skup privatnih ključeva (d1, n1; d2, n2) i javnih ključeva (e1, n1; e2, n2).
9. Postupak u skladu s Patentnim zahtjevom 5, **naznačen time**, da za vrijeme kodiranja, zadnji modul (A1) koristi tzv. javni ključ (e2, n2), a za vrijeme dekodiranja, prvi modul (A2) koristi tzv. privatni ključ (d2, n2).
10. Postupak u skladu s Patentnim zahtjevima 1 do 3, **naznačen time**, da uključuje tri modula za kodiranje/dekodiranje (A1, A, A2) s asimetričnim ključevima.

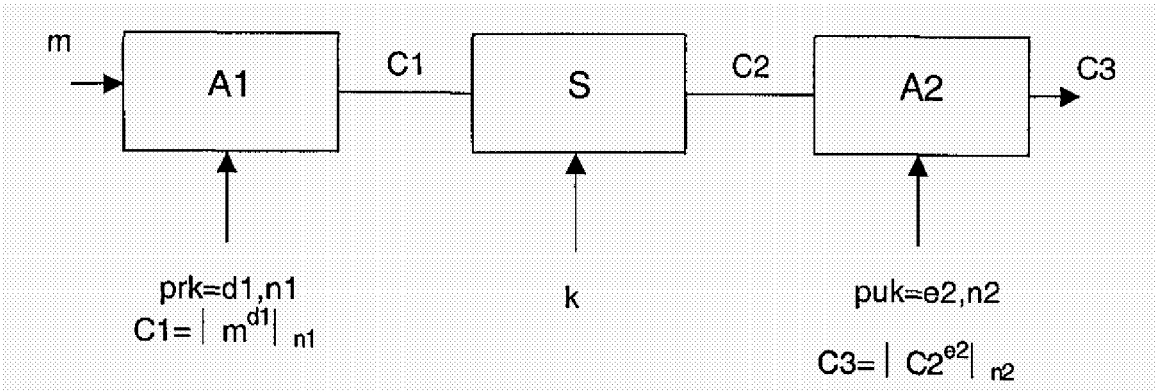
SAŽETAK

Kada se koristi modul za kodiranje/dekodiranje, postoje postupci za određivanje ključa ili ključeva koje koristi modul i to putem analize podataka koji ulaze ili izlaze iz modula. U svrhu uklanjanja tog nedostatka, predloženi višemodulni postupak uključuje modul koji započinje svoje operacije kodiranja/dekodiranja čim dobije na raspolaganje dio rezultata iz modula prije njega (gledano u smjeru toka podataka).

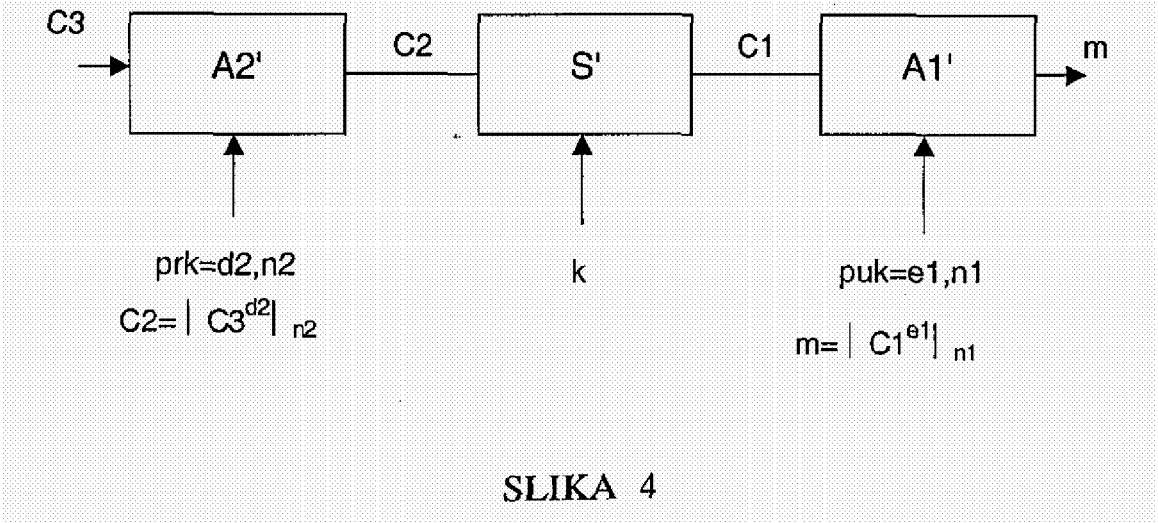


SLIKA 1

SLIKA 2



SLIKA 3



SLIKA 4