

AUTENTIFIKACIJA

Autentifikacija poruka

- Za informaciju se kaže da je autentična ako je:
 - Nepromenjena
 - Zaista potiče od navodnog izvora

Autentifikacija poruka moguća je:

- Pomoću konvencionalnog šifrovanja
- Bez šifrovanja
 - Kod za autentifikaciju poruke
 - Heš funkcija za jednosmerno šifrovanje

Autentifikacija pomoću konvencionalnog šifrovanja

- Simetrično šifrovanje nije pogodno za autentifikaciju – u nekim režimima šifrovanja moguće je da napadač promeni redosled blokova šifrata
- Svaki blok će se uspešno dešifrovati, ali promena redosleda može da promeni značenje celokupne informacije

Autentifikacija bez šifrovanja poruke

- Najčešće se autentifikacija obezbeđuje zasebno od šifrovanja poruka

Kod za autentifikaciju poruke

- Pomoću tajnog ključa generiše se mali blok podataka koji se zove kod za autentifikaciju poruke (MAC-message authentication cod)
- Poruka i kod se prenose
- Pošiljalac i primalac znaju tajni ključ
- Primalac iz primljene poruke izračunava kod pomoću tajnog ključa i poredi izračunati kod sa primljenim kodom
- Uobičajeno kod sadrži 16 ili 32 bita

Autentifikacija bez šifrovanja poruke

Heš funkcija za jednosmerno šifrovanje

- Od poruke promenljive dužine M , pravi izvod poruke $H(M)$, bez korišćenja tajnog ključa
- Izvod poruke (heš) može se šifrovati tajnim ili javnim ključem, a može se i pri pravljenju izvoda koristiti tajna vrednost koja se ne prenosi već se doda na izlazu zbog izračunavanja kontrolnog izvoda koji se poredi sa prenetim izvodom
- Ako se izvod (heš) šifruje, na prijemu se porede heš koji se dobija računanjem iz pristigle poruke i heš koji je primljen i dešifrovan

Heš funkcija za jednosmerno šifrovanje

- Kada se koristi javni ključ:
 - Osim autentifikacije dobija se i digitalni potpis
 - Nema distribucije ključeva

Elektronsko potpisivanje

- E-mail
 - E- trgovina
 - Finansijske transakcije
-
- Provera identiteta pošiljaoca
 - Integritet poruke
 - Neporecivost

Bezbedne Hash funkcije

- Šifarski sistemi sa javnim ključevima, kao i sistemi za digitalni potpis mogu biti veoma spori.
- Takođe, u nekim slučajevima, dužina digitalnog potpisa može biti veća ili jednaka dužini same poruke koja se potpisuje.
- Da bi se rešili ovi problemi koriste se hash funkcije.

- Hash funkcija je izračunljiva funkcija koja primenjena na poruku m promenljive dužine daje njen rezime (otisak) fiksne dužine koja se naziva njenom hash vrednošću - $H(m)$
- Hash funkcije se definišu na sledeći način:

$$H : M \rightarrow M \qquad H(m) = h$$

- U opštem slučaju, $H(m)$ je mnogo manjih dimenzija od m . Na primer, m može da ima dužinu od jednog megabajta, dok $H(m)$ može imati svega 128 ili 160 bita.

- Upotrebom hash funkcija, problem dužine poruke ili digitalnog potpisa se rešava tako što se umesto da se šifruje ili digitalno potpisuje cela poruka m , potpisuje se ili šifruje samo rezime poruke – $H(m)$
- Hash funkcije koje su se najviše koristile u kriptografske svrhe su MD2, MD4 i MD5 (Message Digest), koje je predložio Rivest. Ove funkcije daju rezimee dužine 128 bita.
- Pored njih, bila je popularna i SHA-1 (Secure Hash Algorithm) funkcija (NIST) koja daje otisak poruke dužine 160 bita.
- Sve navedene funkcije su razbijene od strane kriptanalitičara

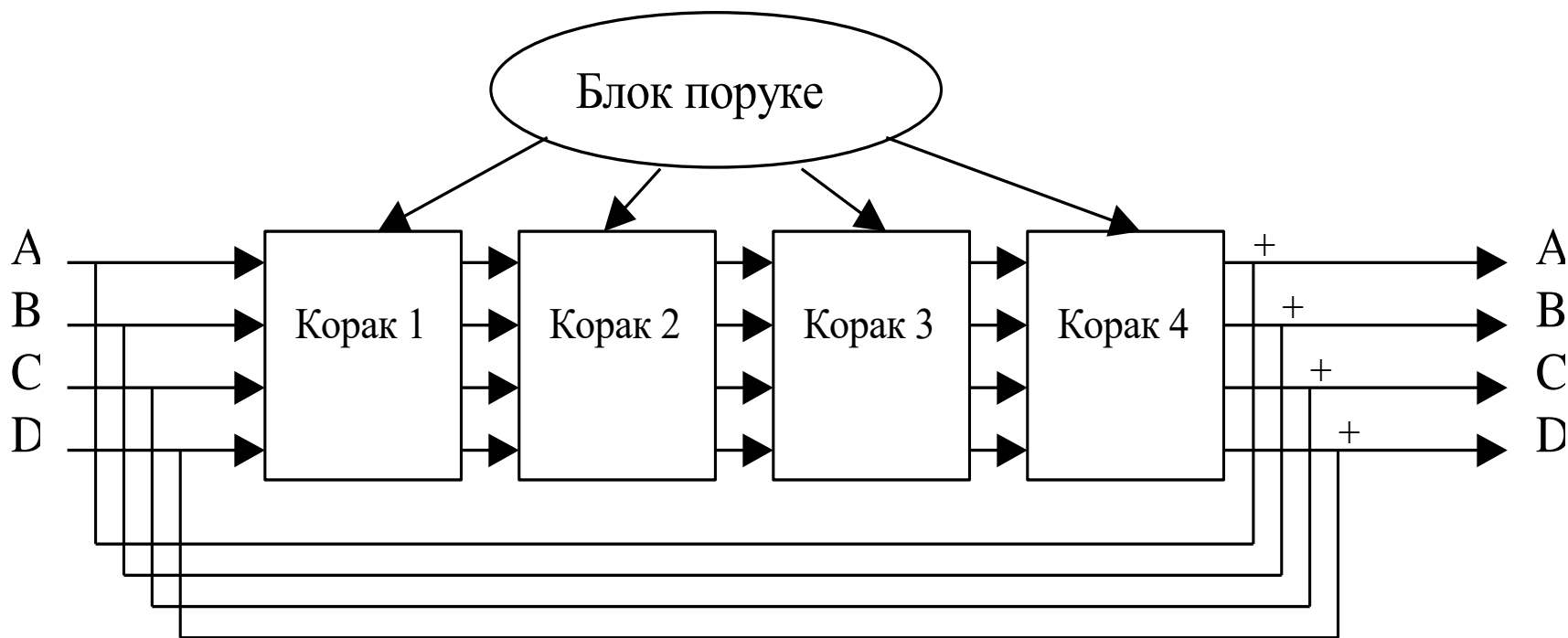
MD5 algoritam

- Proizvodi 128-bitnu heš vrednost poruke
- Ulazna poruka se deli na blokove od 512 bita
- Blokovi se dele u podblokove po 32 bita (16)
- Sažetak poruke se postavi na 4 podbloka dužine po 32 bita i formira se 128-bitna heš vrednost

MD5 algoritam

- Dodavanje bita za dopunjavanje
 - Poruka se proširuje tako da bude tačno za 64 bita kraća od celobrojnog multipla 512 bita – prvo se na kraj poruke doda jedan bit jedinice, a onda se doda potreban broj nula
- Dopunjavanje dužine
 - 64 bita koji predstavljaju dužinu poruke, dodaju se na kraju
- Inicijalizacija MD bafera
 - Inicijalizuju se 4 promenljive A, B, C i D dužine po 32 bita
 - AA, BB, CC i DD
- Definisanje 4 nelinearne funkcije
 - F, G, H i I - ulaz su 4 32-bitne reči, izlaz takođe
- Transformacija za 4 kruga
 - Glavna petlja algoritma izvršava se za sve blokove poruke u 4 kruga (faze)
- Proračun 4 kruga (64 koraka)
 - Svaki krug ima različite operacije - FF, GG, HH i II, 16 puta
- Rezultat su 4 bloka po 32 bita

MD5 algoritam



SHA-1 algoritam

Algoritam se sastoji od sledećih koraka:

1. Prvo se poruka obradi tako da je njena dužina tačno multipl od 512 bita
2. Zatim se inicijalizuju 5 32-bitne promenljive
3. Zatim počinje glavna petlja algoritma koja se izvršava za sve blokove dužine 512 bita date poruke.

SHA - 2

- Ovo je revidirana verzija standarda SHA-1
- Definisane su tri nove SHA-256, SHA-384 i SHA-512 sa dužinama heša 256, 384 i 512 bita
- Koriste se blokovi od po 1024 bita
- Dodaje se 128 bita koji sadrže dužinu originalne poruke
- Izlaz je 512 bita za haš vrednost
- Svaki bit heš koda je funkcija svakog ulaznog bita
- SHA 3 zvanično objavljen 2012. god

Kodovi za autentifikaciju poruka

Postoji značajno zanimanje za razvoj MAC-a izvedenog iz heš koda poput SHA-1 iz bar dva razloga:

- Heš funkcije se uglavnom izvršavaju brže od konvencionalnih algoritama za šifrovanje
- Kod za heš funkcije je svuda dostupan

Heš funkcija ne može da se direktno koristi kao MAC jer se ne oslanja na tajni ključ, ali moguća je ugradnja tajnog ključa u postojeći heš algoritam

HMAC

- Koristi se u raznim Internet protokolima:
 - IP security
 - TLS (Transport Layer Security)
 - SET (Secure Electronic Transaction)
- Koristi raspoložive heš funkcije bez modifikacija (kao modul)
- Ugrađenu heš funkciju je lako zameniti bržom ili bezbednijom, ako je potrebno
- Ključ dopunjen potrebnim brojem nula XOR-uje se sa nekim definisanim nizom bita, pa se to provlači kroz heš funkciju i generiše se ključ

Šifarski sistemi

- Šifarski sistem tajnim ključem je familija parova funkcija (E_k, D_k) za svaki ključ k iz skupa ključeva K , definisana na sledeći način:

$$E_k : M \rightarrow X$$

$$D_k : X \rightarrow M$$

- M i X su skupovi otvorenih tekstova i šifrata, respektivno
- Za svaki otvoreni tekst m iz M važi:

$$D_k(E_k(m)) = m$$

- Da bi se koristio ovakav sistem, korisnici A i B se dogovore da uzmu tajni ključ k iz K . Ako A želi da pošalje poruku m iz M korisniku B, šifruje je pomoću funkcije E_k , $E_k(m) = c$ i rezultat c se šalje korisniku B.
- Da bi rekonstruisao originalnu poruku, B dešifruje primljeni šifrat c pomoću funkcije D_k ,

$$D_k(c) = D_k(E_k(m)) = m$$

Problemi u kriptografiji sa tajnim ključevima

- Distribucija ključeva – dva korisnika moraju da izaberu tajni ključ pre početka komunikacije i da za njegovo prenošenje koriste siguran kanal. Ovakav siguran kanal nije uvek na raspolaganju.

Problemi u kriptografiji sa tajnim ključevima

- **Manipulacija ključevima** – U mreži sa n korisnika, svaki par korisnika mora da ima svoj sopstveni tajni ključ, što čini ukupno $n(n-1)/2$ ključeva za tu mrežu.
- **Nemogućnost realizacije procedure digitalnog potpisa**– U šifarskim sistemima sa tajnim ključevima nema mogućnosti, u opštem slučaju, za digitalno potpisivanje poruka, tako da onaj koji prima poruku ne može da bude siguran da je onaj koji mu je poslao poruku zaista njen autor.