# Kodovi za autentifikaciju poruka (MACs)

Prirodno-matematički fakultet, Podgorica
Mentor: Dr Vladimir Božović
Student: Vladimir Peković

Specijalistički rad
Maj, 2013.

# Uvod

- Kako znati da poruka nije putem izmijenjena?
- Kako znati da je sagovornik onaj za koga se predstavlja?
- Integritet podataka garantuje da nije došlo do izmjene sadržaja poruke na njenom putu od izvora do odredišta.
- Autentifikacija je proces u kome se dokazuju identiteti krajnjih elemenata komunikacije.

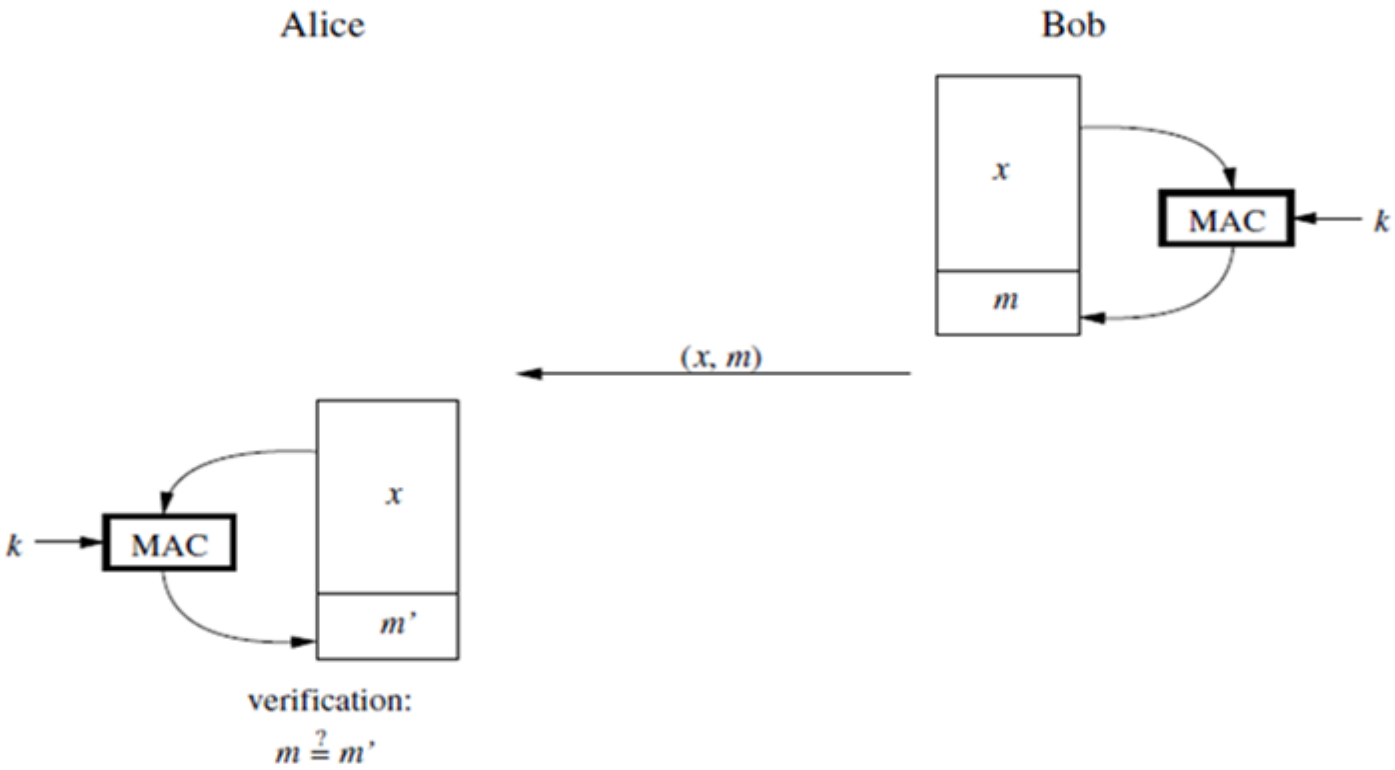
# Šta je MAC?

- Kodovi za autentifikaciju poruka (MAC - Message Authentication Code) predstavljaju niz bita koji se dodaju na originalnu poruku kako bi se obezbijedila autentifikacija pošiljaoca i integritet poruke.
- MAC nije isto što i digitalni potpis.
- MAC se koristi u finansijskim transakcijama, mobilnim komunikacijama (GSM), autentifikaciji internet komunikacija sa SSL/TLS protokolima itd.

# Principi MAC-a

- MAC je funkcija koja zavisi od simetričnog ključa k i poruke x. Koristićemo sledeću notaciju:

$$m = \mathrm{MAC}_k(x).$$



# Principi MAC-a (2)

- Motivacija za korišćenje MAC-a je da Alisa i Bob žele da detektuju bilo koju manipulaciju poruke x prilikom prenosa. Za ovo, Bob izračunava MAC kao funkciju od poruke i dijeljenog tajnog ključa k. On šalje Alisi i poruku x i autentifikovanu oznaku m. Pošto je ovo simetričan proces, Alisa, po prijemu poruke x i autentifikovane oznake m, jednostavno ponavlja korake koje je Bob sprovodio prilikom slanja poruke: ponovo proračunava autentifikovanu oznaku pomoću poruke x i dijeljenog tajnog ključa k i provjerava da li se slaže sa Bobovim m.
- Osnovna pretpostavka ovog sistema je da će MAC-ovo računanje dovesti do netačnog rezultata ako je poruka x promijenjena u toku prenosa.

# Principi MAC-a (3)

- MAC algoritmi su familija funkcija $f_k$ parametrizovanih tajnim ključem k, sa sledećim svojstvima:
  1. lakoća izračunavanja - za poznatu funkciju $f_k$, sa zadatim vrijednostima k i ulaza x, $f_k(x)$ je lako izračunati.
  2. kompresija - $f_k$ preslikava ulaz proizvoljne konačne dužine na izlaz $f_k(x)$ određene dužine n.
  3. funkcija preslikavanja je sirjektivna (potencijalno mnoge poruke imaju isti MAC) - nalaženje takvih poruka sa identičnim MAC-om mora da bude teško.

# Realizacija MAC-a

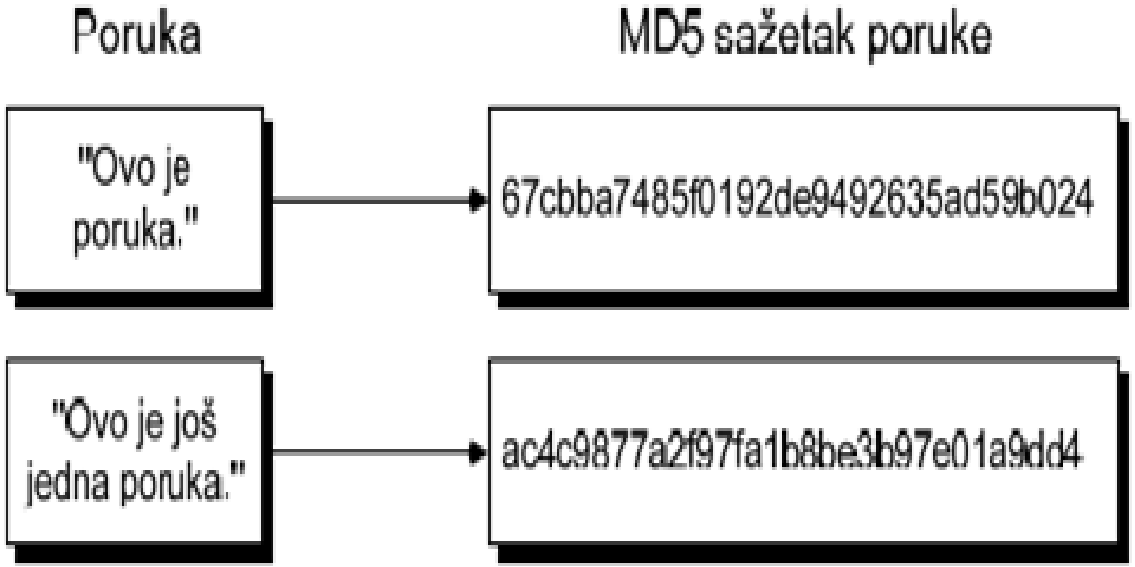
- U praksi, MAC je zasnovan ili na blok šiframa ili heš funkcijama.
- HMAC (Hash-based Message Authentication Code) - koristi se neki od poznatih heš algoritama u realizaciji MAC algoritma (HMAC-MD5, HMAC-SH1)
- CMAC (Cipher-based Message Authentication Code) – temeljen na algoritmima za kriptovanje blokova.

# MAC iz heš funkcija (HMAC)

- Ukoliko su poruke dugačke, potpisivanje cijele poruke može da bude veoma nepraktično. Kao logično rešenje ovog problema javlja se mogućnost, potpisivanja samo sadržaja umesto potpisivanja cijele poruke.
- Svaka promjena izvorne poruke izaziva promjenu u sadržaju, što se odražava na promjenu potpisa, čime se minimizuje mogućnost zloupotrebe.
- Za kreiranje sadržaja poruke se koristi heš funkcija za sažimanje.

# MAC iz heš funkcija (HMAC) (2)

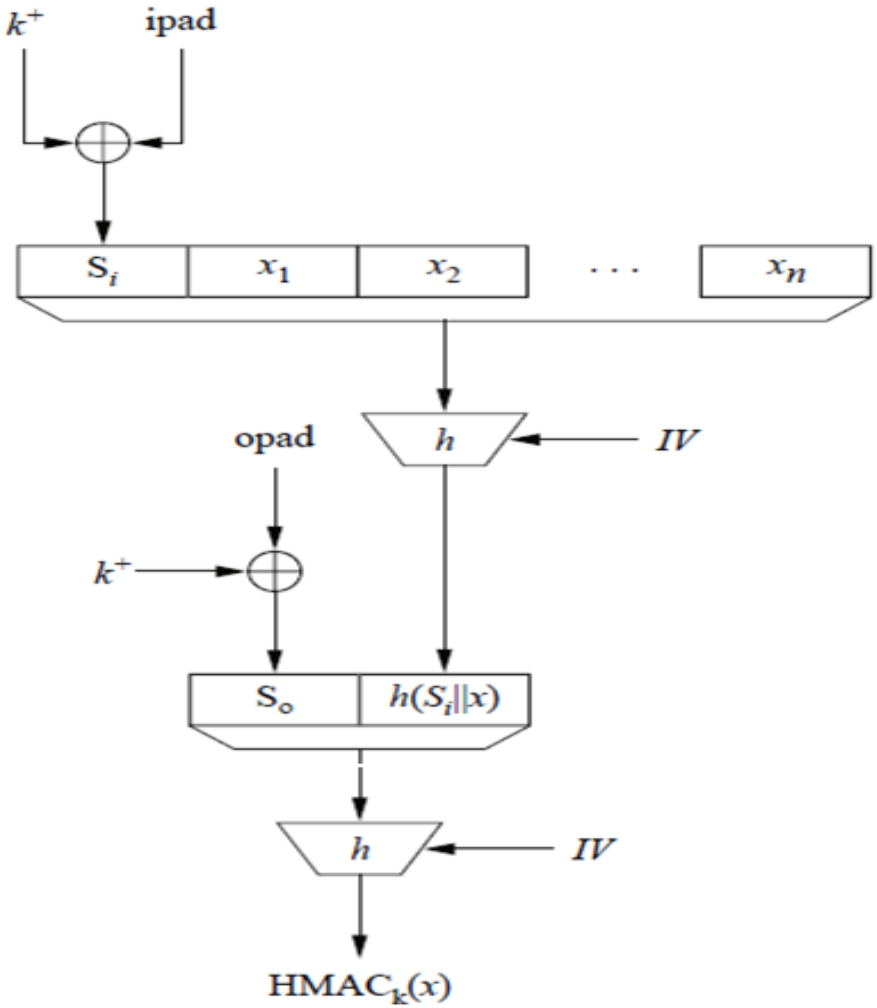
- Osnovna karakteristika heš funkcije je da i najmanja promjena u originalnoj poruci dovodi do promjene njene heš vrijednosti.




- HMAC se može koristiti u kombinaciji s bilo kojom iterativnom funkcijom za izračunavanje sadržaja poruke. MD5 i SHA-1 su primjeri takvih funkcija.

# MAC iz heš funkcija (HMAC) (3)

- Osnovna ideja koja stoji iza svih šifri autentifikiacije poruke koje su zasnovane na hešu je da se ključ hešira zajedno sa porukom.



# MAC iz heš funkcija (HMAC) (4)

- MAC računanje počinje sa proširivanjem simetričnog ključa k sa nulama sa lijeve strane tako da je rezultat ključ $k^+$ dužine b bajtova, gdje je b ulazna širina bloka heš funkcije.
- Na prošireni ključ i na konstntu

  ipad = bajt 0x36 ponovljen 64 puta,

  je primijenjena operacija XOR (ekskluzivno-ILI).
- Izlaz XOR-a formira prvi ulazni blok heš funkcije. Sledeći ulazni blokovi su blokovi poruka $(x_1, x_2, \ldots, x_n)$.
- Drugo, spoljni heš se izračunava sa ključem i izlazom prvog heša. Ovdje, ključ je ponovo proširen sa nulama, a zatim je opet primijenjena operacija XOR sa konstantom

  opad = bajt 0x5C ponovljen 64 puta.

# MAC iz heš funkcija (HMAC) (5)

- Nakon što je spoljašnji heš izračunat, izlaz je šifra autentifikacije poruke od x. HMAC konstrukcija može biti izražena kao:

$$\mathrm{HMAC}_k(\mathrm{x}) = \mathrm{h}[(k^+ \oplus opad) \parallel h\,[(k^+ \oplus ipad) \parallel x]]$$

Hvala na pažnji!