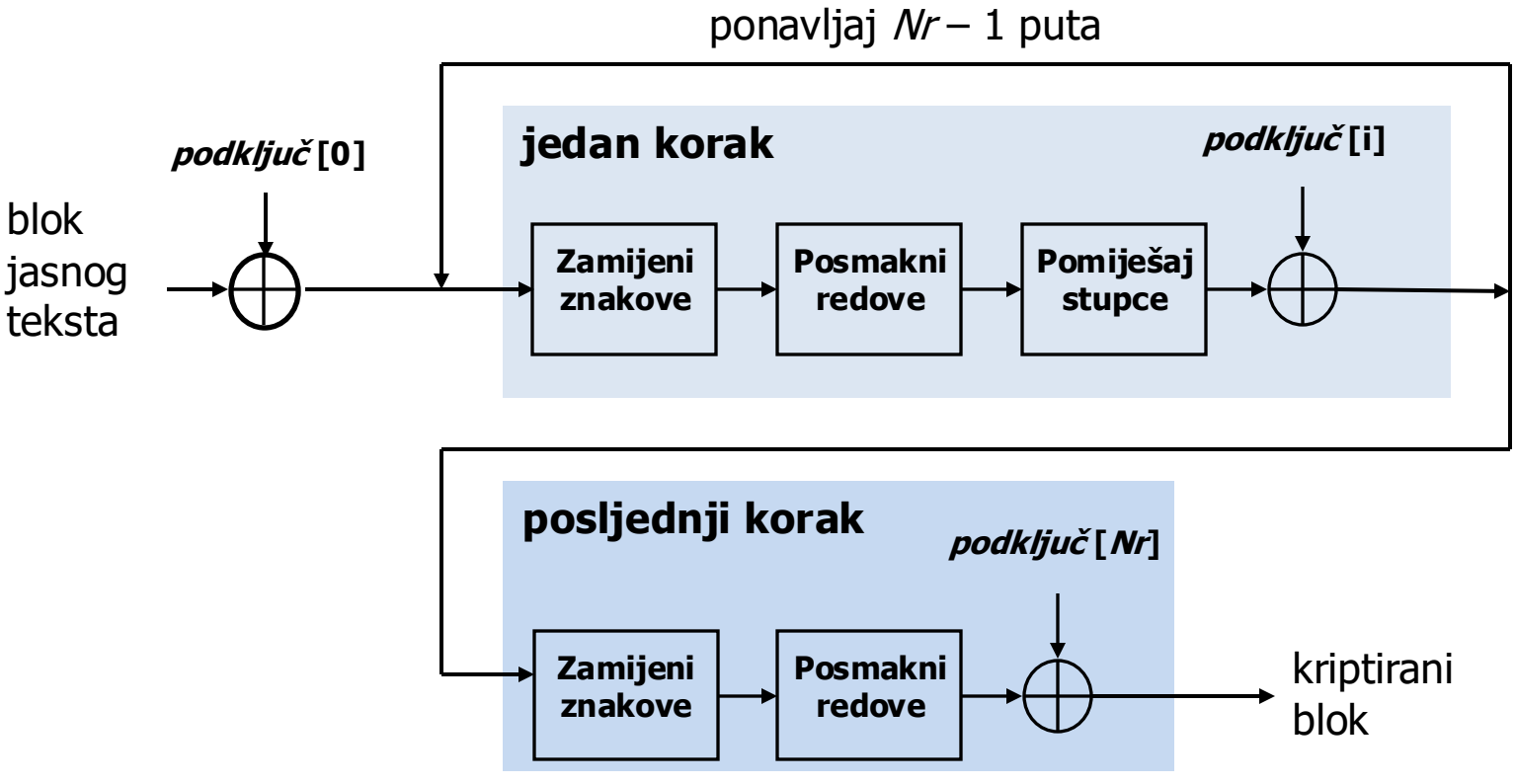
Kriptografija i kriptoanaliza

doc. dr. sc. Ante Đerek i prof. dr. sc. Marin Golub

listopad 2023.

Ponavljanje: AES – postupak kriptiranja



Ponavljanje: konačno polje $GF\ (2^8)$

- elementi polja su polinomi oblika:

  $a_7x^7 + a_6x^6 + \ldots + a_1x + a_0, \qquad a_i \{0, 1\}$

- svaki bajt $a_7a_6a_5a_4a_3a_2a_1a_0$ (niz od 8 bitova) je predstavljen odgovarajućim polinomom

- *zbrajanje* - isključivo ILI
- *množenje* - binarno množenje polinoma modulo fiksni ireducibilni polinom

  $g(x) = x^8 + x^4 + x^3 + x + 1 \equiv 11B_H$

Ponavljanje: Funkcije koje koristi algoritam AES

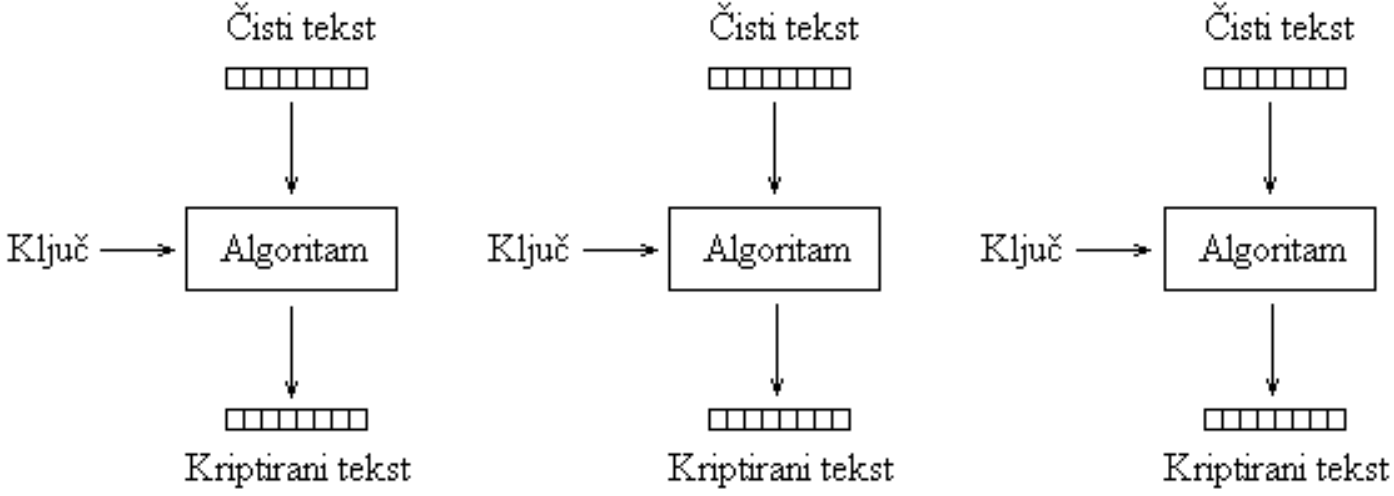
- *pomiješaj stupce*
  - Za svaki stupac bloka računa se stupac novog stanja:

$$\begin{bmatrix} s_{0i}' \\ s_{1i}' \\ s_{2i}' \\ s_{3i}' \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0i} \\ s_{1i} \\ s_{2i} \\ s_{3i} \end{bmatrix}$$

Načini kriptiranja

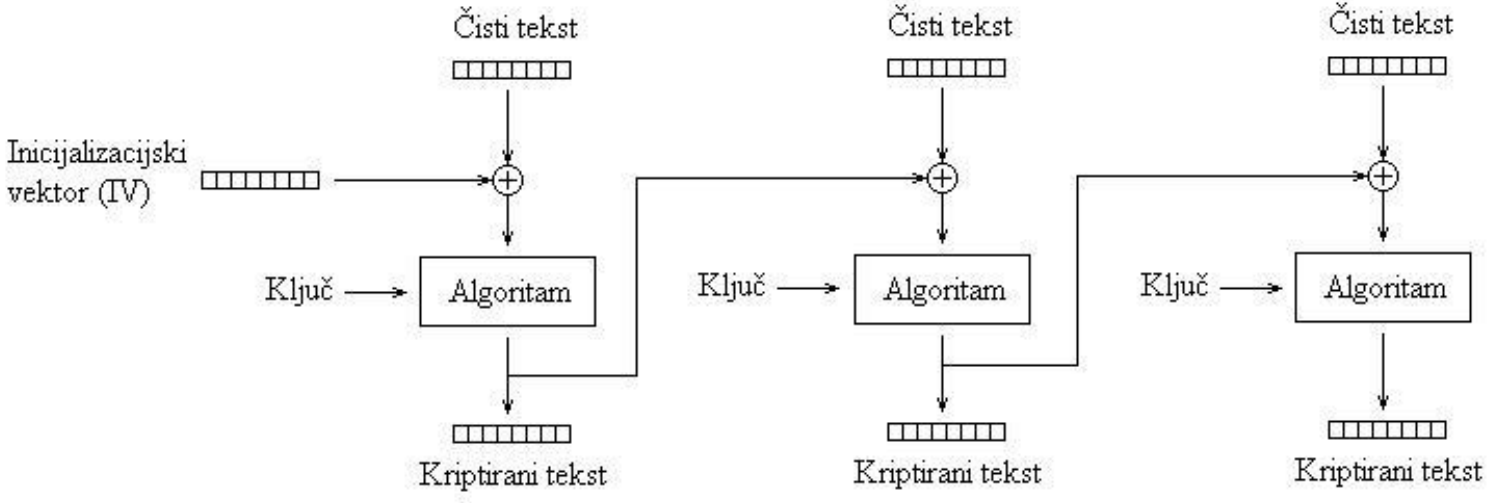
- Želimo kriptirati poruku proizvoljne duljine!
- Želimo jača sigurnosna svojstva koja nam ne može pružiti deterministično kriptiranje!

Načini kriptiranja: ECB - Electronic Codebook



Fakultet elektrotehnike i računarstva

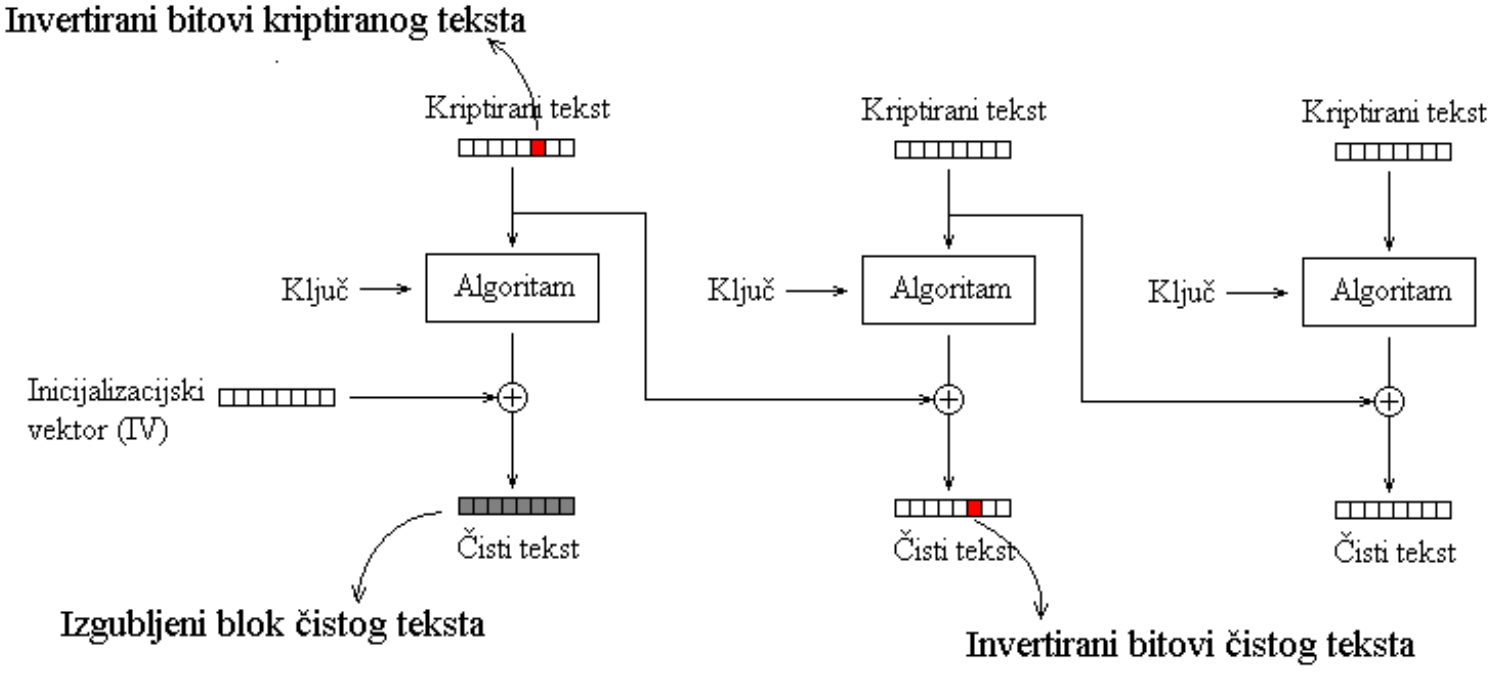
Način kriptiranja: Cipher Block Chaining (CBC)



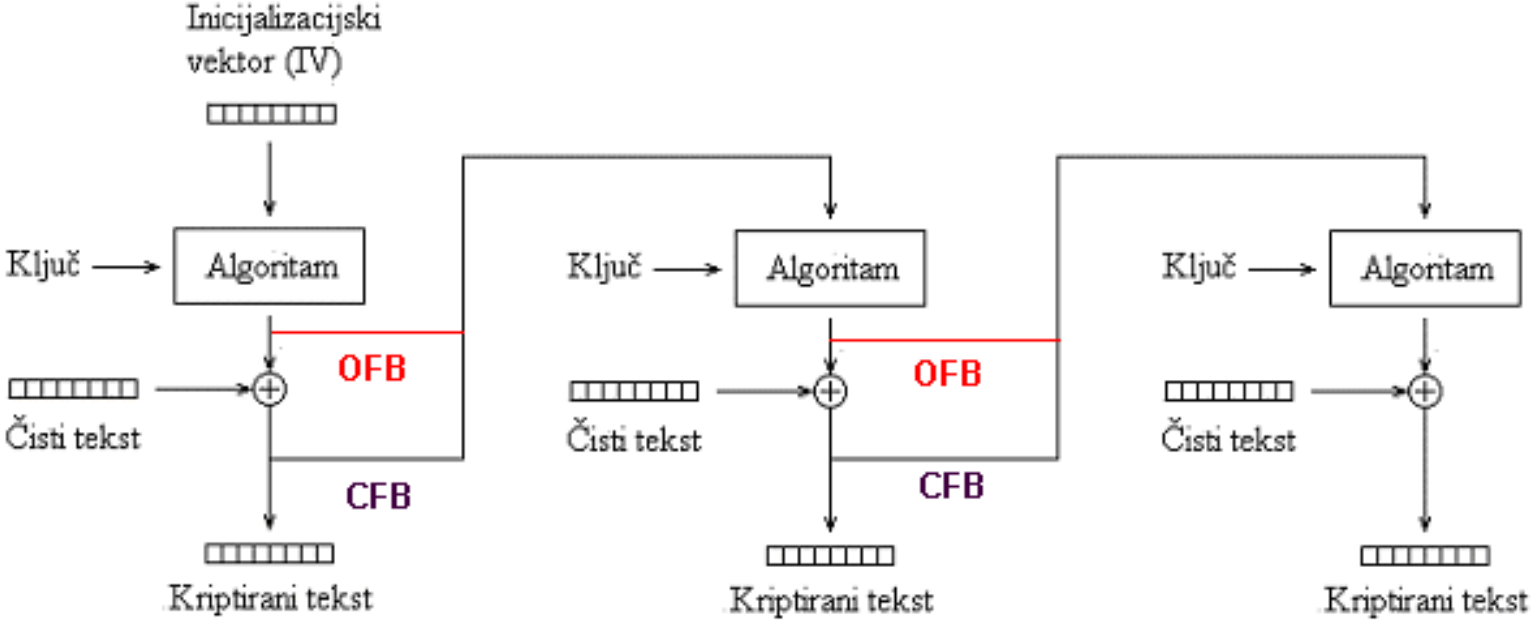
Cipher Block Chaining (CBC)

- Inicijalizacijski vektor IV se mora izabrati nasumično.
- Inicijalizacijski vektor IV se šalje zajedno s skrivenim tekstom (odnosno on je dio skrivenog teksta).
  - Posljedica: IV ne mora (i ne može) biti tajan.
- Potrebno je nadopuniti poruku tako da je duljina višekratnik veličine bloka.
- Kriptiranje: blok kriptiranog teksta ovisi o svim prethodnim blokovima jasnog teksta.
- Dekriptiranje: blok jasnog teksta ovisi o dva susjedna bloka kriptiranog teksta.
- Rezultat je sigurna enkripcija pod razumnim pretpostavkama.

Način kriptiranja: *Cipher Block Chaining (CBC)*



Načini kriptiranja Cipher Feedback (CFB) i Output Feedback (OFB)



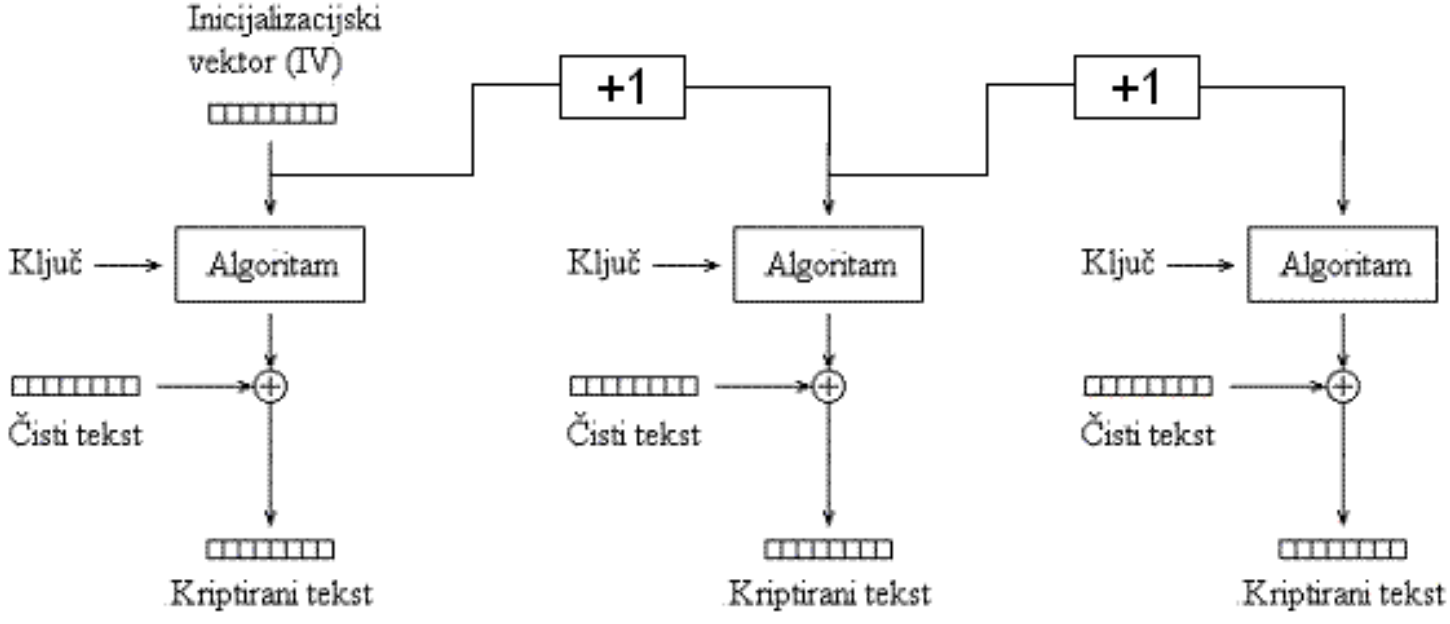
Output Feedback (OFB)

- Sličan protočnoj enkripciji odnosno jednostrukoj bilježnici: na temelju ključa i IV se izračuna niz bitova koji se XOR-a s jasnim tekstom.
- Dekripcija jednaka enkripciji.
- Zadatak: Što se događa ako se isti IV koristi dva puta?

Cipher Feedback (CFB)

- Sličan OFB načinu ali bitovi kojima se XOR-a dodatno ovise o jasnom tekstu.
- Dekripcija vrlo slična enkripciji.

Način kriptiranja *Counter Mode (CTR)*



CTR

- Sličan protočnoj enkripciji odnosno jednostrukoj bilježnici: na temelju ključa i IV se izračuna niz bitova koji se XOR-a s jasnim tekstom.
- Moguće paralelizirati.
- Nije potrebno nadopunjavati poruku.

Nadopunjavanje (padding)

- Kod CBC i nekih drugih načina kriptiranja je potrebno nadopuniti poruku do višekratnika duljine bloka.
- Nadopunjavanje mora biti invertibilno.
- Primjer: PKCSv7

```
          01 -- if lth mod k = k-1
       02 02 -- if lth mod k = k-2
          .
          .
          .
k k ... k k -- if lth mod k = 0
```

Izvor: https://datatracker.ietf.org/doc/html/rfc5652

Zadatak: *padding oracle* napad

- Jednostavna stvar poput nadopunjavanja može biti izvor sigurnosnih problema!
- Recimo da TLS poslužitelj koristi CBC način s PKCSv7 nadopunjavanjem. Kada TLS poslužitelj primi poruku, on je dekriptira te pokušava ukloniti nadopunjavanje.
  - Vraća „Invalid padding” poruku ako nadopunjavanje nije ispravno.
- Napadač je vidio da klijent poslužitelju šalje poruku (IV, C_0, C_1). Opišite način da napadač dekriptira zadnji blok.

Preporuke

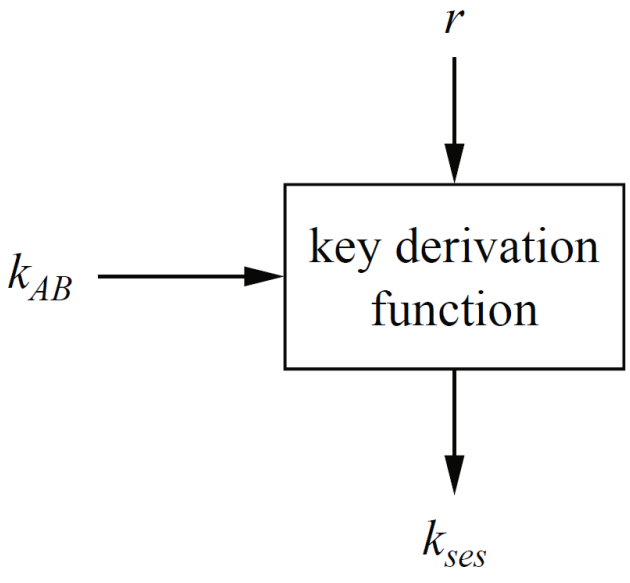
- Koristiti provjerena ostvarenja algoritama
  - NIKAKO se NE preporuča vlastita implementacija
- NE koristiti način kriptiranja ECB.
- IV se ne smije ponavljati i treba ga generirati slučajno (primjerice kod CBC načina kriptiranja)
- NE koristiti stalno isti simetrični ključ

Derivacija ključeva

- Problem: Kako općenito pretvoriti „tajne podatke” u ključeve prikladane za simetričnu enkripciju?
  - Kako pretvoriti lozinku u ključ za simetričnu enkripciju?
  - Kako pretvoriti „matematičku” dijeljenu tajnu u ključ za simetričnu enkripciju?
  - Što ako je “procurilo” pola 256-bitnog ključa?
  - Kako generirati više ključeva iz jednoga?

Funkcije za derivaciju ključa

- Funkcija za derivaciju ključa je deterministička funkcija koja kao ulaze prima:
  - Tajnu vrijednost k_{AB}
  - Javni parametar r
- Kao izlaz daje
  - Ključ za simetričnu šifru k_{ses}



Sigurnost funkcija za derivaciju ključa

- Neformalno, funkcija za derivaciju ključa je *sigurna* ako je napadač koji ne zna k_{AB} ne može odrediti nikakve informacije od $k_{ses} = KDF(k_{AB}, r)$
  - čak i ako zna r
  - čak i ako djelomično zna k_{AB}
  - čak i ako zna $KDF(k_{AB}, r_i)$ za mnoge $r_i \neq r$.

Sigurnost funkcija za derivaciju ključa

- Ako je KDF sigurna funkcija za derivaciju ključa onda je jednako teško
  - Saznati k_{AB} u potpunosti
  - Saznati bilo što o k_{ses}
- Posebno, funkcija za derivaciju ključa mora biti *jednosmjerna*.

Primjena: derivacija ključeva iz lozinki

- $k = KDF(lozinka, salt)$
- $salt$ se bira nasumično, ali je nakon toga javan (npr. pohranjuje se zajedno s skrivenim tekstom)
- Obično se koriste *password based* KDF koje su konstruirane tako da budu sporije.
  - PBKDF2
  - Scrypt
  - …

Primjena: derivacija više ključeva iz jednog

- $k_1 = KDF(k_{master}, \text{"Encryption key 1"})$
- $k_2 = KDF(k_{master}, \text{"Encryption key 2"})$
- Alternativno koristi se KDF sa većim izlazom koji se podijeli.

Funkcije za derivaciju ključa – konstrukcije

- Bazirane na hash funkcijama: HKDF
- Bazirane na sustavima kriptiranja bloka
- …

Funkcije za derivaciju ključa – česte greške

- Kriptografska hash funkcija često *nije* dobra funkcija za derivaciju ključa.
  - Npr. $KDF(k_{AB}, r) = SHA256(k_{AB}||r)$
- *Length extension* napad
  - Na temelju $SHA256(x)$ je ponekad moguće izračunati $SHA256(x||x')$

Laboratorijska vježba: double ratchet

- 1. vježba: symmetric key ratchet
- 2. vježba: Diffle-Hellman ratchet

Demo