<RSA> Sigurnost informacijskih sistema </RSA>

<AES> predavanja </AES>

<CISSP> Kriptografija II</CISSP>

```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v2

hQIMA/+lLdj1rKphAQ//Y4frYwEfh92E9o/lXP7hg4JXxw7MOcmSXg5ttoB44cP9
SBqzqnCtul9OjL4xvUFkkmmZx4oO0fFN2jB9pIKM/jyML1MbfOPbAPkr9JGoe0AW
sEBogtXZ8KYSaq9g4m/ukmjemCgoquC6oIZ3YCiuz3nLGdW/9HiXiKsJFEV8GXfA
Uq7Af27bR7uAgKwkIYLvona0Cd2MNSmfyObyYR01nsJXrwOePzS521gYXO/4uNIM
Trb6pg8Hn02e6uExVUyDIb9URCaHMMt0FymigGjhDM30ZERLHe2wJlEZfmim8pb+
nRO6H9ROQ64IOD5LkpCE5JyYQJMNfg2ZUz4jmCSzpGFBF7NpI+hyNwVS4tLmmKtO
eB+1xSA2kCsNmcQUxpUijUJFGV4RtxCRlJSYoiXlfve4jhP/RdlX/WHI0UfzEu9v
One4k1yPPJ8lnKK5KQBLiOVEv8/b8s6burTi3yv5y00jEMy7L84zhIPdjBvU9dhn
UfdS2S+PlD/Ur+oK2vcgpuMHHMMCrEhr4wk+2estuEtDI5+1SmbG5ckfG0nl9P0Q
/hCAAkwDy9biHTZokuklkQHdCPViL+fHWndHX4SQ6GTdnDToSfT19S5li6mqF9gR
B5NB9IpHHPFgN9YNQ10AJnqDdmEfnxRucR/QeOuOG7hLgK/yjjpFkJk0yp6Anf/S
uQEEMSHpZI2NuDlSCQPDb4JThdWM0RKmRF/Si/kVqxL2h19o5cDcx8kd4QUDsmdK
2fHRfhngn2Y8Viq7zm/vK9CTm1MLkC/eWmDIKRLcZ27T3IT7Mu4eEFYX+EIZM2FL
QAREtIS/uDd4hBlhqsKx8pFHkB32433S6wO8wByfXDy7PN3yhU1PNNinnaNK1lpL
D+cYeVpJV4+4mJ5XY2yNozcw+24+3V2NQPbwtxyPGIRsipY+XySzWtuB
=x47A
-----END PGP MESSAGE-----
```

Summary

- Činjenice
- Simetrična enkripcija
- Asimetrična enkripcija
- Upotreba

Lekcija 1.Činjenice

- Računski „nemoguće“?
- Slučajni generatori bita
- Hash funkcije

Računski „nemoguće“?

- ...mi kažemo računarski.
- Recimo da postoje 10 Ghz procesori.
  - Svaki košta 10 KM
- U jednom taktu mogu testirati 100 ključeva
- Za 10 miliona KM možemo napraviti mašinu koja testira 10^{18} ključeva po sekundi.
- Takva hipotetička mašina bi mogla probiti 80-bitni ključ za 7 dana.
- Međutim, za 128 bitni ključ bi trebalo 10^{12} godina
- Oko 100x više nego procijenjena starost svemira

Slučajni generatori bita

- Slučajni generatori su važni, prisutni i neophodni u svim modernim kriptografskim algoritmima.
- Cilj je da pronalaženje *seed* vrijednosti bude netrivijalan zadatak.
- Primjeri:
  - Poseban hardver
  - Korisnička aktivnost (tastatura i miš);
  - Aktivnost hardvera (cpu, temperatura, disk)
  - Šum iz analogno/digitalnih konvertora (zvuk, kamera)
  - Sadržaj i vrijeme protoka mrežnih paketa
  - Vremenska komponenta

- Sve navedeno su pseudo generatori slučajnih vrijednosti

Hash funkcije

- Hash nije enkripcija
  - Ne postoji obrnuti proces
- Služi za provjeru integriteta (podataka, sadržaja i sl.)
- Varijabilni ulaz – fiksni izlaz
- U kriptografiji se koriste sigurne hash funkcije koje obezbjeđuje sljedeće osobine:
  - Jednosmjerna: za vrijednost y je računski nemoguće pronaći x gdje je h(x) = y
  - Otpornost na izmjene. Promjena samo jednog bita na ulazu dovodi do rapidne promjene izlaza
- Poznati primjeri hash funkcija su:
  - MD5 i SHA-a
- 2004 godine je pronađena kolizija u MD5 funkciji
  - http://www.ietf.org/rfc/rfc1321.txt

Lekcija 2.Simetrična enkripcija

- Kriptografija simetričnog ključa
- DES
- DES šema
- 3DES
- AES

Kriptografija simetričnog ključa

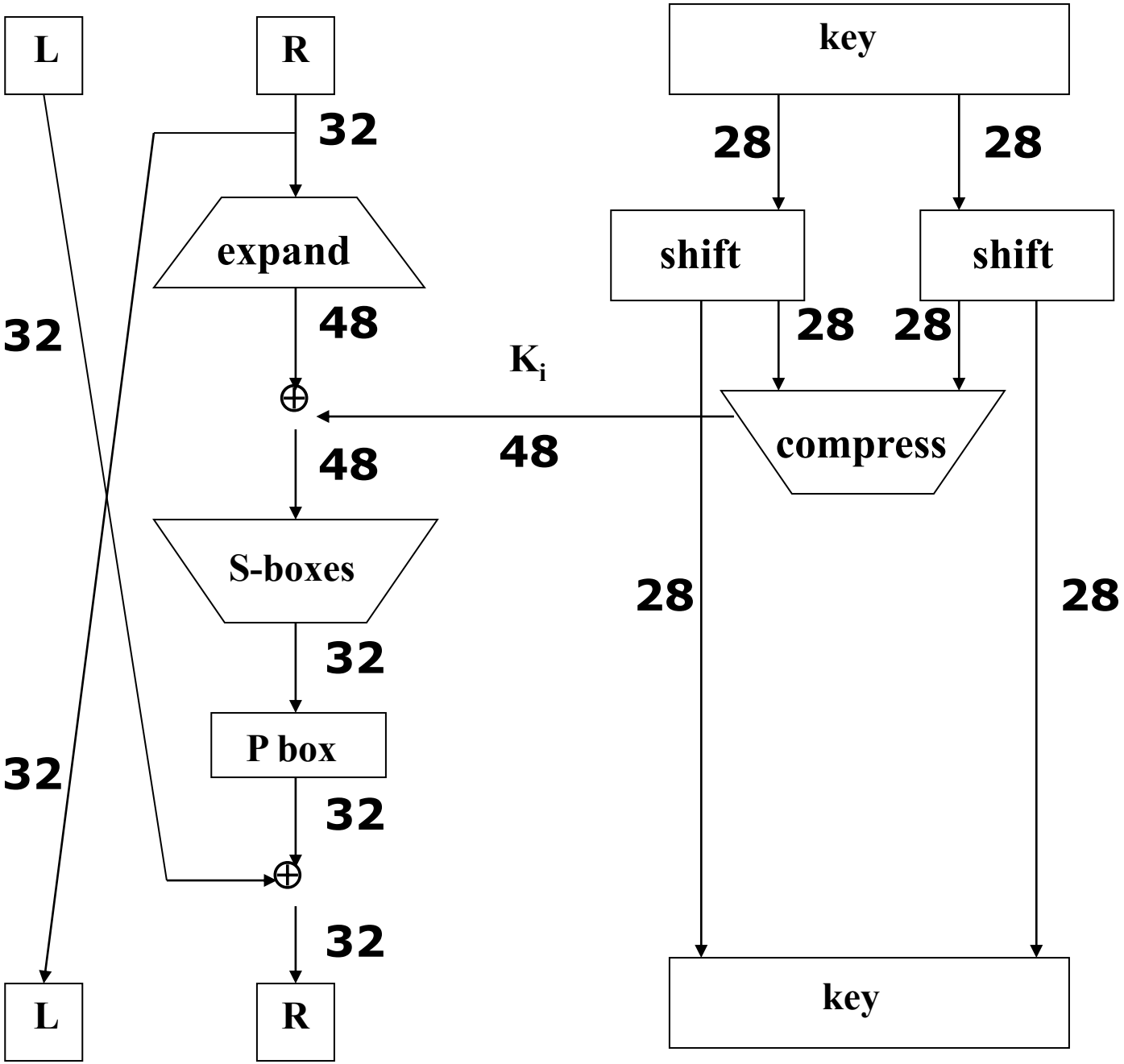
- *Stream cipher* - one-time pad
  - Ključ je relativno „kratak“
  - Provučen kroz *keystream*
  - *Keystream* se koristi na principu one-time pad
- *Block cipher* - baziran na *codebook*
  - *Block cipher* ključ određuje knjigu kodova
  - Svaki ključ dolazi sa drugačijom knjigom kodova
  - Unosi “konfuziju” i “difuziju”

DES-Data Encryption Standard

- DES je razvijen 1975 - IBM
  - 1977 postao standard
  - Oficijelni standard U.S. Vlade
  - Zasnovan na „Lucifer" blok šifri
- Bilo je dosta kontroverzi oko razvoja ovog algoritama
  - NSA je bila umiješana (tajno)
  - Dizajn je bio tajan
  - Dužina ključa je redukovana sa 128 na 56 bita
  - Obilato korišten od strane banaka i velikog broja aplikacija u proteklih 25 godina
- Nasljednici:Triple DES, G-DES, DES-X, LOKI89, ICE

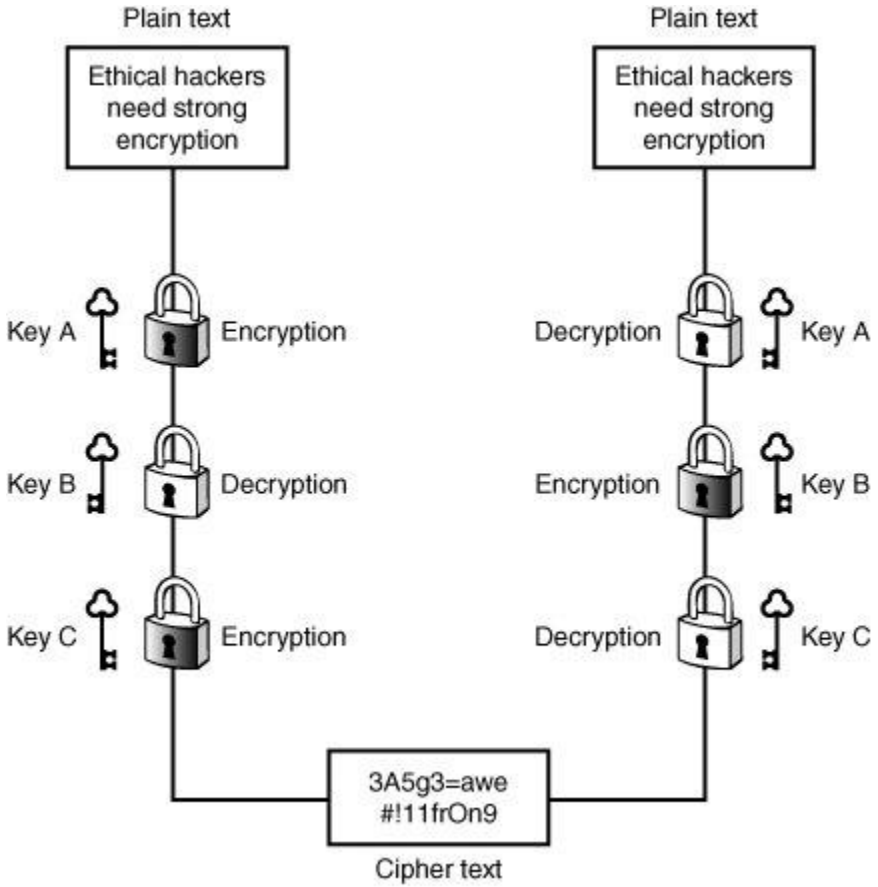
DES šema – jedan ciklus

- DES je šifra sa:
  - 64 bitnom dužinom blokova
  - 56 bitnom dužinom ključa
  - 16 ciklusa ponavljanja
  - 48 bita od ključa se koristi
    - u svakom ciklusu (subkey)



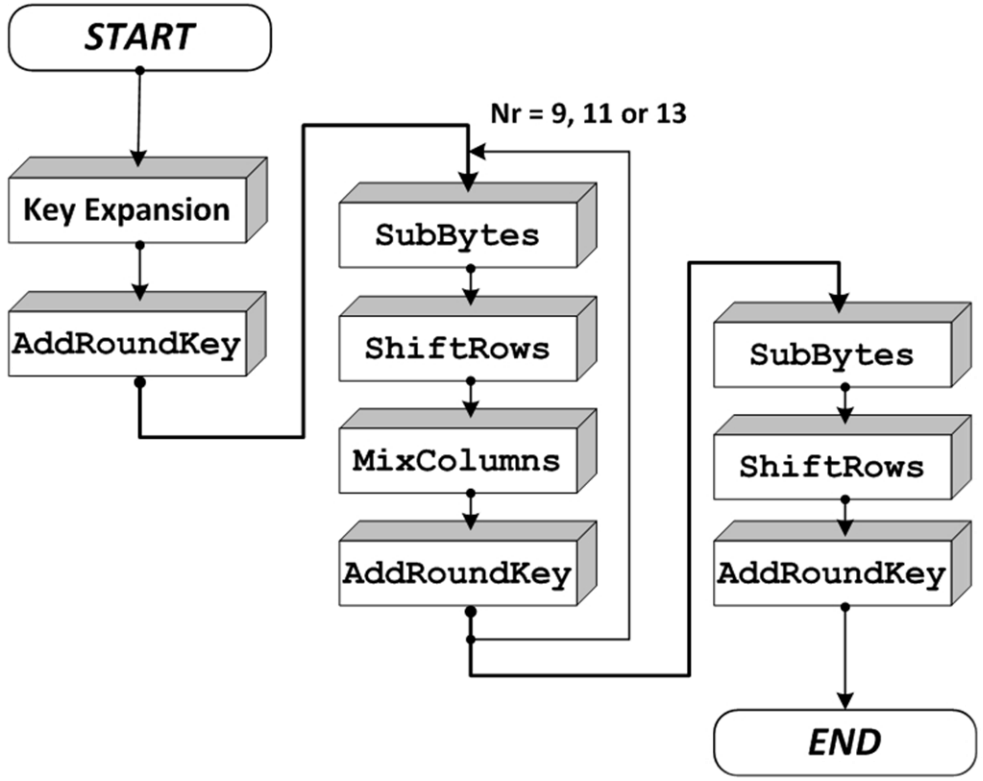
3DES

- Danas, 56 bitni DES ključ je vrlo „slab“
- Napad testiranja svih kombinacija je izvodiv i uspješan
  - Januar 1999
  - Electroni Frontier Fundation distributed.net
  - DES je probijen za 22 sata i 15 minuta
- Rješenje je bilo da se DES osnaži
- Triple DES ili 3DES (112 bitni ključ)



AES – Advanced Encryption Standard

- Efikasnija zamjena za DES
- Autori: Joan Daemen i Vincent Rijme
- Javni i transparetni poziv:
  - NSA otvoreno uključena
  - Predloženi su mnogi jaki algoritmi
  - Odabran je Rijndael algoritam
    - (izgovara se “Rain Doll” ili “Rhine Doll”)
- Iteracijski blokovi kao u DES-a
- Nije baziran na Feistel-ovoj šifri
- Veličina bloka je 128 bita
- Dužina ključa: 128, 192 ili 256 bita
- 10 do 14 ciklusa
  - Svaki ciklus uključuje 4 funkcije



Lekcija 3. Asimetrična enkripcija

- Kriptografija javnog ključa
- RSA
- RSA činjenice
- Generisanje ključa
- Diffie-Hellmanov protokol za razmjenu ključeva

Kriptografija javnog ključa

- Cilj je postići sigurniji način komunikacije
- Riješiti problem razmjene jednog ključa

RSA

- RSA je najpoznatiji algoritam kriptografije javnim ključem.
- Nazvan je po početnim slovima prezimena svojih pronalazača:
  - **R**ivest, **S**hamir i **A**dleman.
- Sigurnost RSA se zasniva na teškom faktorisanju velikih brojeva.
- Javni i privatni ključ su par velikih, od 100 do 200-cifrenih, prostih brojeva:

33478071698956898786044169848212690817704794983713768568912431388982883793878002287614711652531743087737814467999489

* *3674604366679959042824463379962795263227915816434308764267603228381573966651127923337341714339681027009279873630891 7*

= *1230186684530117755130494958384962720772853569595334792197322452151726400507263657518745202199786469389956474942774063845925192557326303453731548268507917026122142913461670429214311602221240479274737794080665351419597459856902143413*

Dužina u bitima: 768 **Decimalna dužina: 232**

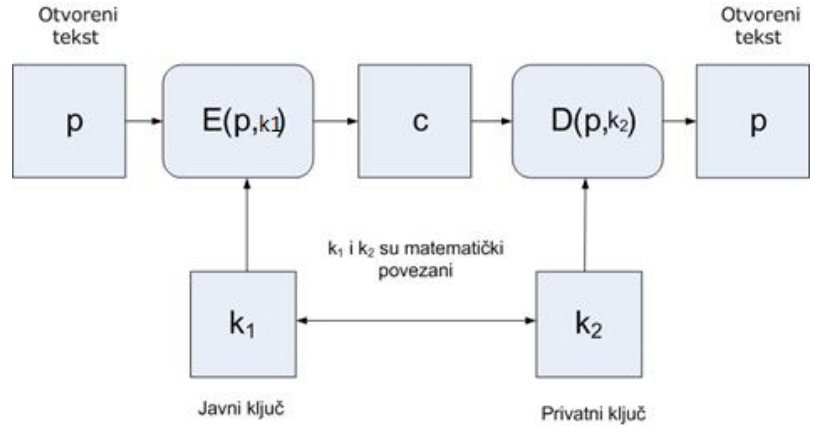
- Trenutno se faktorizacija broja od 80 cifara radi brzo
- RSA koristi brojeve od najmanje 300 cifara

RSA činjenice

- Sistem je potpuno baziran na primjeni pojedinih matematičkim konecepata:

1. **Modul operator**
2. **Euler –totientova funkcija**
3. **Euler-Fermat teorema**

Generisanje ključeva



Formalna definicija

1. Choose two primes p and q with $p \neq q$
2. Calculate their product: $N = p * q$
3. Calculate the value of Euler's totient function of N

$$\varphi(N) = \varphi(p * q) = (p-1)(q-1)$$

4. Choose a number e between 1 and $N-1$ which is coprime to $\varphi(N)$
5. Find another number d where

$$d * e \equiv 1 \; mod \; \varphi(N)$$

Primjer

1. Suppose we select $p = 13$ and $q = 7$
2. Thus: $N = 13 * 7 = 91$
3. $\varphi(91) = \varphi(13 * 7) = (13-1)(7-1) = 72$
4. Suppose we choose $e = 5$, because:
   $gcd(5, 72) = 1$
5. We will select $d = 29$ as thus:
   $d * e = 145 = 2 * 72 + 1 \equiv 1 \; mod \; 72$

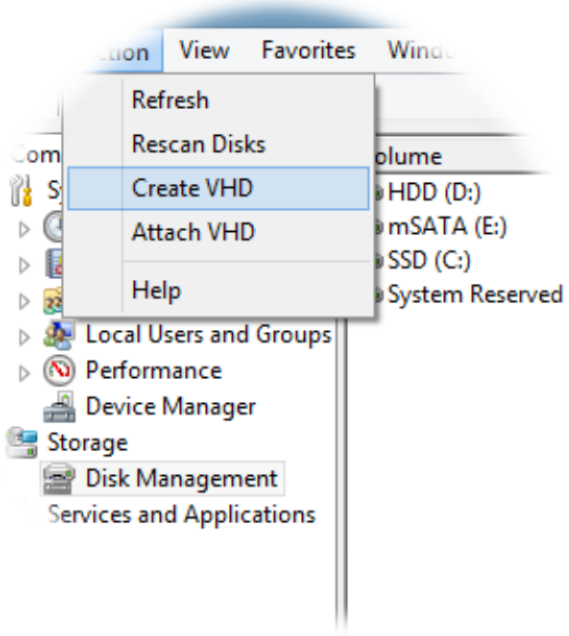
(e, N) je *javni RSA ključ.*
(d, N) je *privatni ključ.*

Diffie-Hellmanov protokol za razmjenu ključeva

- Distribucija ključeva je jedna od najslabijih tačaka ne samo ovog sistema šifrovanja, već i svih kriptosistema uopšte
- Diffie i Hellman (1976), dva istraživača sa Stanforda, predložili su rješenje problema razmjene ključeva
- Ovaj protokol obuhvata sljedeće korake:
- Korisnik A bira slučajan veliki broj x i šalje korisniku B $X = g^x \bmod n$
- B bira slučajan veliki broj y i šalje A $Y = g^y \bmod n$
- A određuje $k = Y^x \bmod n$
- B određuje $k' = X^y \bmod n$

Upotreba

- Enkripcija fajlova
- Enkripcija diskova
- Enkripcija email poruka
- HTTPS
- Chat enkripcija (end2end)
- Anonimno surfanja



Pitanja