Adatbiztonság és kriptográfia Név: SIKLÓSI BÁLINT

NagyZH, 2016. április 7.

1. Mond ki és bizonyítsd a kis Fermat tételt.

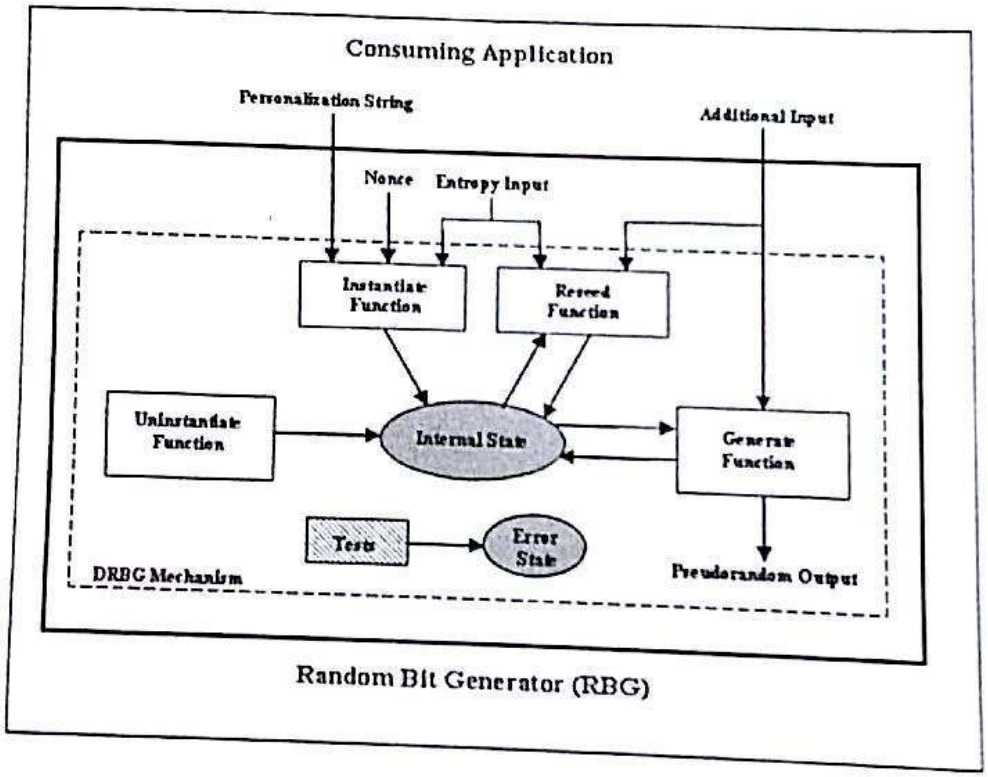
T.: p - prím, a és p relatív prímek

$$a^{p-1} = 1 \pmod p$$

B.: $r \cdot a$ és $s \cdot a$ ugyanannyi maradékot ad p-vel osztva.

$$ra \equiv sa \pmod p$$
$$r = s \pmod p$$
$$\Downarrow$$
$$a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1)a = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \pmod p$$
$$a^{p-1}(p-1)! = (p-1)! \pmod p$$
$$a^{p-1} = 1 \pmod p$$

2. Az ábra segítségével magyarázd el a korszerű véletlenszám generátorok elvi működését?

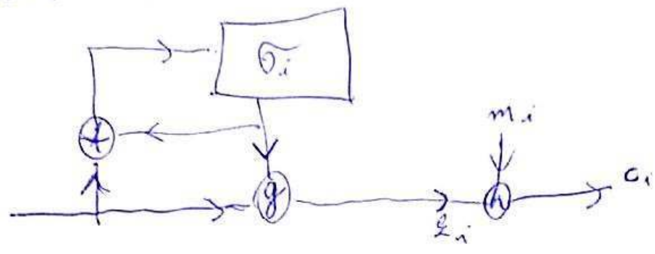


Nonce → egyedi érték

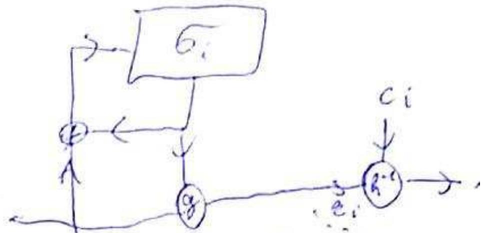
Entropy input → [illegible]

3. Mi a szinkron adatfolyam rejtjelezők általános modellje (kódolás és dekódolás ábrája és magyarázata)?

kódol:



dekódol:



kulcs generálás, majd titkosítás (pl. h = XOR)

kulcs generálás majd azonos módon : ... vissz... az ere...

* →

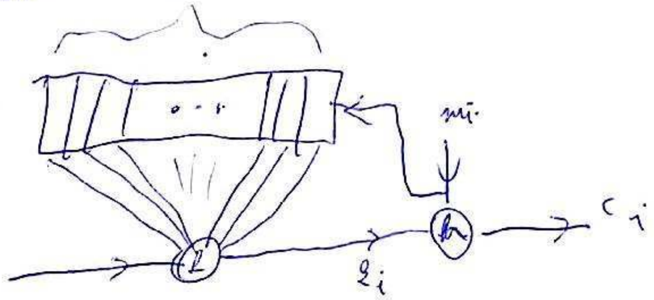
σ_i ~> aktuális belső állapot

*~> k_i ~> kulcs
m_i ~> nyílt üzenet
c_i ~> titkos üzenet

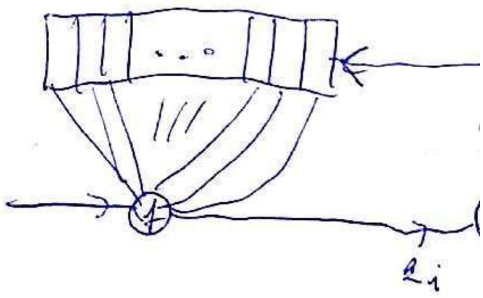
4. Mi az önszinkronizáló adatfolyam rejtjelezők általános modellje (kódolás és dekódolás ábrája és magyarázata)? Az önszinkronizáló adatfolyam rejtjelező esetén mi biztosítja a szinkronitást a kódoló és dekódoló fél között? Mi történik egy bithiba (bit értékének megváltozása, ill. egy bit elvesztése) esetén?

*↘

kódol: m db



dekódol:



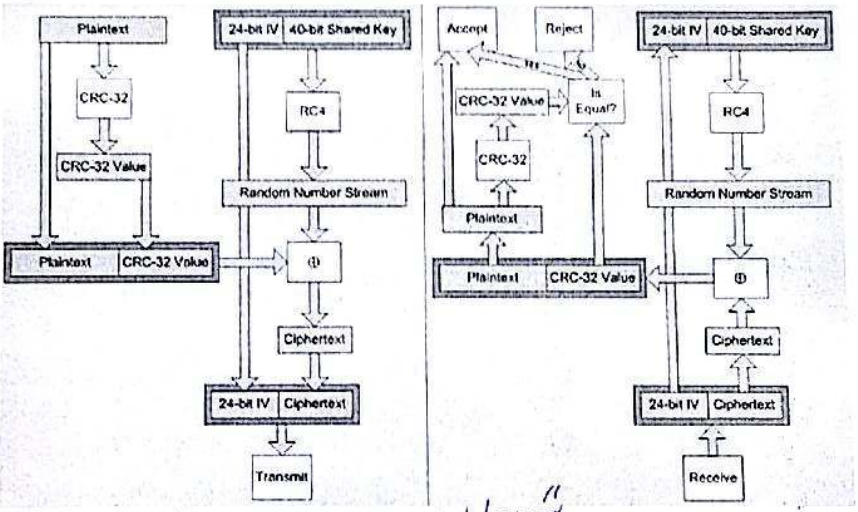
A korábbi üzenetek felhasználásával kódol/dekód...
Az azonos kezdeti érték biztosítja a szinkront.
Bithiba esetén annyi csomag fog hibásan átérni ...
... üzenet elem szükséges a kód/dekód-hoz (n

Adatbiztonság és kriptográfia Név: SIKLÓSI BÁLINT

5. A 802.11 szabvány szerint mi a Shared Key Authentication folyamata és az miért sérülékeny? Miért nem engedélyezett a titkosítás nélküli kommunikáció ebben az esetben? 1 /12

Azonos kulcsot használ mind a két fél. Egyetlen titkosítás nélküli üzenet felhasználásával megfejthető a használt kulcs, majd így az összes titkosított üzenet is.

6. Magyarázd el a WEP titkosítási eljárás folyamatát az ábra alapján! Hogyan hozható létre érvényes rejtjelezett üzenet a nyílt üzenet ismerete nélkül amiatt, hogy a CRC-32 lenyomat lineáris leképezés. 5 /12



Adó

1. nyílt szövegről készít egy lenyomatot.
2. A nyílt szöveget és a lenyomatot titkosítja:
   - Rejtjelkulcs,
     + random generálás
   - IV maggal.
3. a titkosított üzenetből a hozzá szükséges magot elküldi

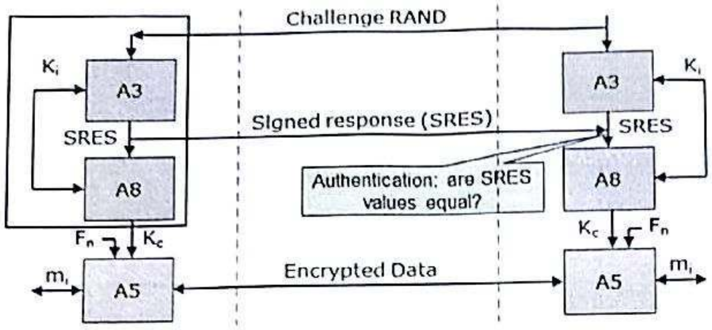
Vevő

1. fogad egy titkosított üzenetet és a hozzá tartozó magot.
2. A visszafejti az titkosított üzenetből az eredeti szöveget és a hozzá tartozó lenyomatot. Ehhez a rejtjelkulcsot és a kapott magot használja.
3. A nyílt szövegről készít egy lenyomatot ugyanazzal az eljárással mint az adó.

Ha a két lenyomat egyezik, elfogadja az üzenetet, különben nem.

5

7. Mi látható az ábrán? Kik a kommunikáló felek? Mi az egyes dobozok, betűk, nyilak tartalma, értelme? Írd le a folyamatot.



folyamat:
1. véletlen generált szá[m]
2. mindkét oldal "nagy ... műveletet végez el (K_i ...) majd visszaküldi a kapott értéket. (SRE[S]
3. Ha a két SRES azo[nos] minden OK, különben csak kell kezdeni.
4. Ha minden OK, akkor ... oldal előállítja azt a ... amivel titkosan ... majd kommunikálni

GSM kommunikáció titkosítása.

felek: – mobil eszköz

– BSC ~ Base Switching Center

8. Hajts végre Diffie-Hellman kulcsegyeztetést A és B között. A modulus: 7, a generátorelem: 3. A és B titkos paramétere tetszőleges, egymástól különböző, 2 és 6 közötti szám legyen.

A: $a = 2$

$p = 7$, $\gamma = 3$

B: $b = 3$

$\alpha = 3^2 \pmod 7 = 2$ ← β → α — $\beta = 3^3 \pmod 7 = 6$

$\beta^a = 6^2 \pmod 7 = 1$ — $\alpha^b = 2^3 \pmod 7 = 1$

x	1	2	3	4	5	6
$3^x \pmod 7$	3	2	6	4	5	1
$2^x \pmod 7$	2	4	1	2	4	1
$6^x \pmod 7$	6	1	6	1	6	1

kulcs = 1

9. Mi a biztosítéka annak, hogy a valóságban (nagy modulus esetén) az egyeztetett Diffie-Hellman kulcs kívülálló számára nem meghatározható? Mi a hatványozás és a diszkrét logaritmus számítás számítási komplexitása?

Így van a kívülálló ismeri γ, p, α, β-t, de a kód visszaf[ejtéséhez] szükséges ismernie a-t, b-t.

$$\text{kulcs} = \gamma^{ab} \pmod p = \gamma^{ba} \pmod p$$
$$\alpha^b \qquad \beta^a$$

Összes pontszám 40

Hatványozni könnyű és egyértelmű.
Logaritmust vonni diszkrét esetben nem lehet, mert ...

$\log_2 1 = 3 \pmod 7$

6, ...