

Név:
Neptun kód:

1.	2.	3.	4.	5.	Σ

ADATBIZTONSÁG ZÁRTHELYI

2010. május 6.

1. Tekintsünk egy mini RSA rejtjelezést $p_1=23$, $p_2=71$ prímeikkel.
 - a) Hány olyan x üzenet van ($1 \leq x < m=p_1p_2$), amelynek nincs közös faktora a titkos prímeikkel? (6 p)
 - b) Mekkora a valószínűsége, hogy egy véletlenszerű x üzenet m faktorizációjára ad lehetőséget? (8 p)
 - c) Adja meg a d kódoló kitevőt, ha $e = 3$ a publikus kitevő! (8 p)
2. Tekintsük az alábbi $H(x, n) = h_1^{(n)}(h_2^{(n)}(x))$ hash függvényt, ahol $h_1^{(n)}$ illetve $h_2^{(n)}$ a h_1 illetve h_2 hash függvények n -szeres alkalmazását jelenti. Milyen feltételek mellett, n mely értékeire lesz biztonságos a $H(x, n)$ konstrukció, ha tudjuk, hogy
 - a) h_1 ütközés-ellenálló, de h_2 nem ütközés-ellenálló tulajdonságú? (8 p)
 - b) h_1 nem ütközés-ellenálló, de h_2 ütközés-ellenálló tulajdonságú? (8 p)Válaszát, mindkét esetben Indokolja!
3. Biometria azonosítás
 - a) Milyen tulajdonságokkal kell rendelkeznie egy emberi fiziológiai vagy viselkedési jellemzőnek ahhoz, hogy alkalmas legyen biometria azonosításra? (4 p)
 - b) Soroljon fel legalább 5 biometria azonosítási módszert! (3 p)
 - c) Milyen típusú ujjlenyomat minutiák léteznek és milyen paraméterekkel reprezentálják ezeket? (3 p)
 - d) Milyen makroszkopikus ujjlenyomat mintázatok léteznek? Soroljon fel legalább hármat! (3 p)
 - e) Ismertesse a minutia alapú matching eljárást! (4 p)
 - f) Milyen típusú hibákkal kell számolni a matching során? Mit jelentenek ezek a hiba fogalmak? (3 p)
4. Tekintsünk egy szervert és két klienst, A -t és B -t. A kliensek azonos valószínűséggel bocsátanak ki kéréseket a szerver felé. A kliensek egymást segítve próbálják anonimizálni a szervernek küldött kéréseiket a következő módon:
 - A a kéréseit p_A valószínűséggel B -n keresztül, $1-p_A$ valószínűséggel közvetlenül küldi a szervernek,
 - B a kéréseit p_B valószínűséggel A -n keresztül, $1-p_B$ valószínűséggel közvetlenül küldi a szervernek.
 - a) Mi a feltétele annak, hogy a fenti rendszer elérje a „gyanún felüli” (beyond suspicion) küldő anonimitási szintet a szerverrel szemben? (10 p)
 - b) Mekkora a szerverrel szembeni küldő anonimitás szintje bitekben mérve (entrópia) ha $p_A = p_B = \frac{1}{4}$ (10 p)

5. Rövid kérdések: ezeket ITT válaszolja meg!

a) Mi a DoS amplification támadás nagyon röviden? (4 p)

b) Milyen kategóriákba sorolhatjuk a lehetséges DoS védekezési módszereket? (3 p)

c) Adjon definíciót a *-tulajdonságra a Bell-LaPadula (BLP) modellben. (3 p)

d) Mi a spam ellenes greylisting lényege? (3 p)

e) Mondjon három TCP flag-et amire egy tűzfalban szűrő szabályt szokás építeni! (3 p)

f) Mi a célja a portscannelésnek? (3 p)

g) Adott két tűzfalszabály:

udp any 192.168.1.0/24 accept

udp 172.16.1.0/24 192.168.1.0/24 deny

Az órai definíciók szerint ez milyen típusú tűzfal inkonzisztencia problémát jelent? (3 p)

Pontozás: 1: <=39, 2: 40 – 54, 3: 55 – 69 , 4: 70 – 84, 5: 85 – 100

MEGOLDÁS

1.

a) $\Phi(m)=22*70=1540$

b) 0.057

$$P = \frac{m - \Phi(m)}{m} = 1 - \frac{(p_1 - 1)(p_2 - 1)}{p_1 p_2} = 1 - \frac{(p_1 p_2 - p_1 - p_2 + 1)}{p_1 p_2} = \frac{1}{p_1} + \frac{1}{p_2} - \frac{1}{p_1 p_2}$$

c) $1540=513*3+1 \rightarrow (-513) \cdot 3=(-1) \cdot 1540+1 \rightarrow d=-513=1027 \pmod{1540}$

2.

a) Semmilyen n-re nem lesz biztonságos, mivel a belső hash leképezésre könnyű ütközést előállítani, amit a külső leképezés helyben hagy.

b) Ha h_2 nem ősképp ellenálló, akkor H nem biztonságos. Indirekt. h_1 nem CRHF így könnyen találunk h_1 -ősképp párt. Ha h_2 nem ősképp ellenálló, akkor ezen párhoz könnyű találni h_2 -ősképp (=H-ősképp) párt.

3.

a) Szükséges tulajdonságok:

- minden ember rendelkezzen az adott jellemzővel (universality)
- az adott jellemző értéke különbözzön különböző emberekre (uniqueness)
- a jellemző ne változzon nagyon időben (permanence)
- a jellemző legyen jól mérhető (collectability)
- legyen nehéz hamisítani (circumvention)

b) ujjlenyomat, irisz minta, arc, fül geometria, renehártya (retina) képe, kéz geometria, hang, arc hőterképe, billentyű-leütés dinamikája, kézi aláírás dinamikája és zaja

c) végződés (ending) és elágazás (bifurcation), paraméterek: a minutia típusa, pozíció X, Y koordinátája, és a minutia szöge

d) íves (arch), hurkos (loop), örvény (whorl)

e) Az ujjlenyomat matching azt próbálja meg eldönteni, hogy két ujjlenyomat azonos ujjról származik-e. A minutia alapú matching 4 lépésből áll:

- minutia párok közötti hasonlóság számolása
- két ujjlenyomat egymásra igazítása a leghasonlóbb minutia párok alapján
- összetartozó (matching) minutiák azonosítása
- globális hasonlósági mérték számolása a két ujjlenyomat között az összetartozó minutiák száma alapján. Ha a hasonlósági mérték egy küszöbszám felett van, akkor a két ujjlenyomat egyezik.

f) Hamis negatív / hamis visszautasítás / Type I: azonos ujjról származó két ujjlenyomat visszautasítása. Hamis pozitív / hamis elfogadás / Type II: különböző ujjakról származó két ujjlenyomat elfogadása egyezőnek

4. a

Jelöljük az eredeti küldőt α -val, és azt a hosztot akitől a szerver a kérést megkapja ω -val.

$$\begin{aligned}\Pr\{\alpha = A|\omega = A\} &= \frac{\Pr\{\omega = A|\alpha = A\} \Pr\{\alpha = A\}}{\sum_{X \in \{A,B\}} \Pr\{\omega = A|\alpha = X\} \Pr\{\alpha = X\}} \\ &= \frac{\Pr\{\omega = A|\alpha = A\}}{\sum_{X \in \{A,B\}} \Pr\{\omega = A|\alpha = X\}} \\ &= \frac{1 - p_A}{1 - p_A + p_B}\end{aligned}$$

Hasonlóan:

$$\begin{aligned}\Pr\{\alpha = B|\omega = A\} &= \frac{p_B}{1 - p_A + p_B} \\ \Pr\{\alpha = B|\omega = B\} &= \frac{1 - p_B}{1 - p_B + p_A} \\ \Pr\{\alpha = A|\omega = B\} &= \frac{p_A}{1 - p_B + p_A}\end{aligned}$$

A gyanún felüli anonimitási szint elérésének feltétele a következő:

$$\begin{aligned}\Pr\{\alpha = A|\omega = A\} &= \Pr\{\alpha = B|\omega = A\} \\ \Pr\{\alpha = B|\omega = B\} &= \Pr\{\alpha = A|\omega = B\}\end{aligned}$$

Ez akkor és csak akkor teljesül, ha $p_A + p_B = 1$.

Ha $p_A = p_B = \frac{1}{4}$, akkor

$$\begin{aligned}\Pr\{\alpha = A|\omega = A\} &= 1 - p_A = \frac{3}{4} \\ \Pr\{\alpha = B|\omega = A\} &= p_B = \frac{1}{4}\end{aligned}$$

Ebből az entrópia a következő módon számolható:

$$\begin{aligned}H &= - \sum_{X \in \{A,B\}} \Pr\{\alpha = X|\omega = A\} \log \Pr\{\alpha = X|\omega = A\} \\ &= -\frac{1}{4} \log \frac{1}{4} - \frac{3}{4} \log \frac{3}{4} \\ &= 0.25 * 2 + 0.75 * 0.415 \\ &= 0.81125\end{aligned}$$

5.

- a) A kérésre vagy sokkal nagyobb válasz, vagy több válasz érkezik, így nagyobb támadás érhető el kisebb befektetéssel. DNS esetén akár 60-70x sávszélesség emészthető fel.
- b) prevention, detection and filtering, traceback and identification.

- c) *-property: for all $(S_i, O_j, \text{append})$ in b , $fc(S_i) \leq fo(O_j)$ and for all (S_i, O_j, write) in b , $fc(S_i) = fo(O_j)$ a subject at a given security level must not write to any object at a lower security level (no write-down). The *-property is also known as the Confinement property.
- d) adott email forrás, cél, forrás ip hármastól nem fogadunk el első alkalomra leveleket.
- e) SYN, FIN, ACK, RST, (URGENT, ECN, CWR-Reduced, Push)
- f) Tipikusan az aktuálisan használt TCP/UDP portok feltérképezése, az esetleges tűzfal szűrések kiderítése, a támadható szolgáltatások felderítése.
- g) shadowing, árnyékolás