**Introduction to Cryptography, Fall 2015**


- **Prof.Dr. Ferucio Laurentiu Tiplea**

**Department of Computer Science**
**"Al.I.Cuza" University of Iaşi**
**C 301**
**Tel: (0232) 201538**


Date: Feb 12, 2016

# Examen Restanţă

1. Schema Fiat-Shamir de identificare are următoarea descriere:

   - **Stabilirea parametrilor.** Se generează două numere prime distincte $p$ şi $q$, se calculează $n = pq$ şi se alege un parametru de securitate $t$. Numerele $p$ şi $q$ sunt secrete, iar $n$ şi $t$ sunt publice;
   - **Alegerea unei valori de identificare.** Entitatea $A$ alege un parametru secret $s \in \mathbf{Z}_n^*$ şi face publică valoarea $v = (s^2)^{-1}\ mod\ n$ (se ştie că este intractabil a determina $s$ cunoscând $v$ şi $n$);
   - **Protocolul de identificare.** Dacă $A$ doreşte să se identifice faţă de $B$, atunci el va repeta de $t$ ori următorul protocol:
     (1) $A$ alege aleator un număr $r$, calculează $x = r^2\ mod\ n$ şi trimite $x$ lui $B$;
     (2) $B$ alege aleator un bit $b \in \{0, 1\}$ şi îl trimite lui $A$;
     (3) $A$ calculează $y = rs^b\ mod\ n$ şi trimite $y$ lui $B$;
     (4) dacă $y^2v^b \not\equiv x\ mod\ n$ atunci $B$ respinge demonstraţia de identitate a lui $A$ şi abortează protocolul.

     Dacă protocolul nu a fost abortat în nici una din cele $t$ iteraţii atunci, după ultima iteraţie, $B$ acceptă demonstraţia de identitate a lui $A$.

   Arătaţi următoarele:

   (a) Dacă $A$ şi $B$ urmează întocmai schema Fiat-Shamir, atunci $B$ va accepta demonstraţia de identitate a lui $A$. **1p**

   (b) Dacă în două iteraţii distincte ale protocolului entitatea $A$ generează acelaşi parametru $r$ inversabil modulo $n$, iar $B$ generează biţi diferiţi (în pasul (2)) în aceste iteraţii, atunci orice intrus care poate obţine informaţiile ce circulă între $A$ şi $B$ poate determina parametrul secret $s$ al lui $A$ în timp polinomial determinist. **1p**

   (c) Orice terţă parte $C$ se poate identifica către $B$ ca fiind $A$ cu probabilitatea $1/2^t$. **1p**

2. Problema *Cinei criptografilor* se formulează astfel. Trei criptografi, $C_1$, $C_2$ şi $C_3$ au luat cina şi, la sfârşit, au fost anunţaţi că cineva a plătit. Masa putea fi plătită de un criptograf (şi doar de unul) atunci când acesta pleca de la masa pentru o perioada scurtă (dar fără a spue celorlalţi că el a plătit-o) sau de o persoană externă.

   Criptografii hotărăsc să afle dacă cina a fost plătită de un extern sau de unul dintre ei dar, în cel de-al doilea caz, să nu se divulge identitatea acestuia. Pentru aceasta ei procedează conform următorului protocol, notat $DC(3)$:

   - fiecare criptograf $C_i$ alege random un bit şi îl comunică în mod secret criptografului din stânga sa (criptografii sunt asezaţi la o masă circulară în ordinea $C_1$, $C_2$, $C_3$, de la stânga la dreapta);
   - fiecare criptograf $C_i$ alege bitul 0 dacă nu a plătit masa, şi 1, altfel;
   - fiecare criptograf $C_i$ publică suma modulo 2 ($\oplus$) a celor 3 bits cunoscuţi, notată $z_i$.

   Fiecare criptograf, analizând suma $z_1 \oplus z_2 \oplus z_3$, deduce dacă masa a fost plătită de unul dintre ei sau de un extern.

   (a) Justificaţi corectitudinea concluziei criptografilor (presupunând că criptografii sunt oneşti în cadrul protocolului $DC(3)$). **1p**

(b) Generalizaţi problema de mai sus la cazul a $n \geq 3$ criptografi (protocolul va fi notat $DC(n)$). **1p**

(c) In cadrul protocolului $DC(n)$, $n \geq 3$, presupunem că criptografii $C_{i-1}$ şi $C_{i+1}$ bănuiesc că $C_i$ a plătit masa. Dacă $C_{i-1}$ şi $C_{i+1}$ îşi pun în comun o parte din informaţiile lor private, pot ei stabili dacă $C_i$ a plătit sau nu? Justificaţi răspunsul. (în cadrul notaţiei de mai sus, dacă $i = 1$ atunci $i - 1$ va fi considerat $n$, iar dacă $i = n$ atunci $i + 1$ va fi considerat 1). **1p**

(d) Dacă consideraţi că răspunsul la punctul precedent este pozitiv, cum credeţi că ar putea fi modificat protocolul $DC(n)$ pentru ca vecinii $C_{i-1}$ şi $C_{i+1}$ ai unui criptograf $C_i$, punându-şi în comun o parte din informaţiilor lor private, să nu poată deduce cu certitudine că $C_i$ a plătit sau nu ? **1p**

(e) Protocolul $DC(n)$ are dezavantajul că dacă un criptograf a plătit masa dar cel puţin un alt criptograf $C_i$ nu este onest în publicarea valorii reale (corecte) $z_i$, atunci concluzia desprinsă de criptografi poate fi eronată. Justificaţi aceasta. **1p**

(f) Descrieţi un protocol cu aceeaşi menire ca şi $DC(n)$ dar pentru care, o situaţie ca cea de la punctul precedent nu mai afectează concluzia finală desprinsă de criptografi. **1p**

**Notă**: baza de notare este 1p.