1. fejezet

# Kriptológia

Azonosítás: $A$ valamilyen titkos információval rendelkezik, és azzal azonosítja magát, hogy ezt az információt tudja. Az információ nyilvános párját egy $S$ szolgáltató aláírja, és garantálja, hogy ez tényleg $A$-hoz tartozik.

Az alábbi protokoll T. Okatomo-tól származik, a Schnorr-protokoll módosítása, amivel még azt is tudjuk garantálni, hogy $B$ nem tud meg további információt $A$-tól, akárhányszor is hajtják végre a protokollt. A protokoll a diszkrét logaritmusra épül, legyen $g_1$, $g_2$ mindkettő $q$-adrendű elem $\pmod p$, ezek nyilvánosak. Ami titkos, az olyan $\alpha$, amire $g_1^\alpha = g_2$ (ezt még $S$-nek sem kell tudnia).

**1. lépés** $A$ megszerzi az aláírt információt $S$-től:

$$\begin{aligned} A \to S: &\quad v = g_1^{-a_1} \cdot g_2^{-a_2},\ a_1,\, a_2 \text{ titkos} \\ S \to A: &\quad s = \{A, v\}_S \text{ ( } S \text{ aláírta )} \end{aligned}$$

**2. lépés** $A$ bizonyítja $B$-nek, hogy ő kicsoda:

$$\begin{aligned} A \to B: &\quad \gamma = g_1^{k_1} \cdot g_2^{k_2}, s, A, v \quad (k_1,\, k_2 \text{ véletlen}) \\ B \to A: &\quad r \qquad\qquad\qquad (\ 1 \le r < 2^t\ ) \\ A \to B: &\quad y_1 = k_1 + a_1 r;\ \ y_1 = k_2 + a_2 r \pmod q \\ B: &\quad \gamma \stackrel{?}{=} g_1^{y_1} \cdot g_2^{y_2} \cdot v^r \pmod p \end{aligned}$$

**1.1. Állítás** *$B$-t nem lehet átverni.*

**Bizonyítás** Tegyük fel, hogy $\widetilde{A}$ kitalált egy $\gamma$-t, amire $B$ a második lépésben akármit válaszol, $\widetilde{A}$ nem elhanyagolható valószínűséggel olyan tud mondani a harmadik lépésben, amit $B$ elfogad. Ekkor vannak olyan különböző $r$ és $r'$ értékek, hogy azokra $A$ tud válaszolni, $y_1$ és $y_2$-t, illetve $y_1'$ és $y_2'$-t, amiket $B$ az utolsó lépésben elfogad, vagyis

$$\gamma = g_1^{y_1} \cdot g_2^{y_2} \cdot v^r = g_1^{y_1'} \cdot g_2^{y_2'} \cdot v^{r'}.$$

Ebből pedig

$$v = g_1^{(y_1 - y_1')(r - r')^{-1}} \cdot g_2^{(y_1 - y_1')(r - r')^{-1}} \tag{1}$$

ami azt jelenti, hogy $\widetilde{A}$ és $S$ együtt ki tudnák számítani a $v$ számnak a $g_1$-re vonatkozó diszkrét logaritmusát. ∎

**1.2. Állítás** *A protokoll folyamán $B$ nem tud meg semmit.*

**Bizonyítás** Tegyük fel, hogy $\widetilde{B}$ sokszor beszélget $A$-val, csak a protokollt használják, és $\widetilde{B}$ valamit megtud $A$-tól, aminek eredményeképpen ő nem elhanyagolható valószínűséggel azt tudja magáról állítani, hogy ő $A$, vagyis $\widetilde{A}$-ként felléphet. Ez azt jelenti, hogy csak a beszélgetések alapján $\widetilde{B}$ az (1) alattiak szerint tud olyan $b_1$ és $b_2$ számokat, amikre

$$v = g_1^{-b_1} \cdot g_2^{-b_2}.$$

Állítjuk, hogy az $A$ által tudott $a_1$ és $a_2$ értékek valamint a $\widetilde{B}$ által tudott $b_1$ és $b_2$ értékek csak $1/q$ valószínűséggel eshetnek egybe. Ez azért van, mert nézzük az összes olyan $a_1$, $a_2$ párt, amire $v = g_1^{-a_1} \cdot g_2^{-a_2}$. Az, hogy ezek melyikét használta $A$ a protokoll folyamán, nem derül ki! Ha ugyanis

$$a_1 + a_2 \cdot \alpha = \overline{a}_1 + \overline{a}_2 \cdot \alpha$$

(vagyis $a_1$, $a_2$ valamint $\overline{a}_1$ és $\overline{a}_2$ ugyanabba a csoportba esik) akkor ha $A$ a harmadik lépésben a $k_1$, $k_2$ véletleneket használta, azok helyett $\overline{k}_1$ illetve $\overline{k}_2$ véletlenek lehetségesek úgy, hogy a $B$ által látott $\gamma$ valamint $y_1$ és $y_2$ válaszok ugyanazok legyenek. Ehhez az kell, hogy

$$k_1 + k_2 \cdot \alpha = \overline{k}_1 + \overline{k}_2 \cdot \alpha$$
$$k_1 + a_1 \cdot r = \overline{k}_1 + \overline{a}_1 \cdot r$$
$$k_2 + a_2 \cdot r = \overline{k}_2 + \overline{a}_2 \cdot r$$

Adott $v$, $\gamma$, $r$, $y_1$ és $y_2$ értékek mellett az összes lehetséges $a_1$, $a_2$ mellé egy és csak egy megfelelő $k_1$, $k_2$ található, tehát csak a válaszok alapján még végtelen számítástechnikai kapacitás esetén sem lehet tudni hogy ezek melyikét használta $A$.

Ezek után $A$ és $\widetilde{B}$ összefog és nagy valószínűséggel tudják a *különböző* $a_1$, $a_2$ valamint $b_1$ és $b_2$ párokat, amikre

$$v = g_1^{-a_1} \cdot g_2^{-a_2} \text{ és } v = g_1^{-b_1} \cdot g_2^{-b_2}.$$

Innen könnyű olyan $\beta$-t kiszámolni, amire $g_1^{\beta} = g_2$, vagyis a diszkrét log problémát megoldják. ■

Következő protokollunk Guillou és Quisquater műve, ami az RSA (prímtényezős felbonthatatlanság) alapú. Az $S$ szolgáltató választ egy $n$ összetett számot, és egy $b < n$ prímet. A feltétel az, hogy $x^b$ ismeretében nem lehet kiszámítani $x$-et. $n$, $b$ publikus. Még az $S$ szolgáltatónak sem kell tudnia $n$ felbontását.

Kezdetben $A$ választ egy $u$ titkos számot. Az azonosító megszerzése a következő:

$$\begin{aligned} A \to S: &\quad v = u^{-b} \pmod{n} \\ S \to A: &\quad s = \{A, v\}_S \end{aligned}$$

Ezek után $A$ a következőképpen azonosítja magát:

$$\begin{aligned} A \to B: &\quad \gamma = k^b \pmod{n} \qquad k \text{ titkos} \\ B \to A: &\quad r \qquad 0 < r < b \text{ véletlen} \\ A \to B: &\quad y = k{\cdot}u^r \pmod{n} \\ B: &\quad \gamma \stackrel{?}{=} y^b{\cdot}v^r \pmod{n} \end{aligned}$$

Világos, hogy ha $A$ nem csal, akkor $B$ elfogadja az aláírást. Most ugyanúgy, mint fent, azt bizonyítjuk, hogy $\widetilde{A}$ nem tudja átverni $B$-t. Ha így volna, akkor $\widetilde{A}$ tudna olyan $\gamma$ értéket választani, hogy $B$ különböző $r$ értékeire tud olyat válaszolni, hogy a választ a végén $B$ elfogadja. Vagyis található olyan különböző $r_1$ és $r_2$, amire $\widetilde{A}$ ki tud számítani $y_1$ és $y_2$ számokat, amiket $B$ elfogad, vagyis

$$y_1^b{\cdot}v^{r_1} = y_2^b{\cdot}v^{r_2} \pmod{n}$$

Mivel $\pmod{n}$ tudunk inverzet számítani, kapjuk hogy

$$v^{r_1 - r_2} = \big(y_2/y_1\big)^b \pmod{n}$$

Most legyen $t$ olyan egész, hogy $(r_1 - r_2){\cdot}t$ $b$-vel osztva $-1$ maradékot ad, vagyis $(r_1 - r_2){\cdot}t = \ell b - 1$, ahonnan

$$\begin{aligned} v^{\ell b+1} &= \big(y_2/y_1\big)^{tb} \pmod{n} \\ u^b = v^{-1} &= \big(y_2/y_1\big)^{tb}{\cdot}v^{-\ell b} \pmod{n} \\ u &= \big(y_2/y_1\big)^{t}{\cdot}v^{-\ell} \pmod{n}, \end{aligned}$$

vagyis $u^{-b}$ ismeretében kiszámítottuk $u$-t. Az utolsó lépésben $b$-edik gyököt azért lehet vonni, mert $b$ és $\varphi(n)$ relatív prímek.

Ebben a protokollban nincs feltétlenül szükség az $S$ szerver aláírására, ha az $A$ nyilvános kulcsa, vagyis $v$ az $A$ nevéből valamilyen egyirányú függvénnyel áll elő. Az

$A$ titkos kulcsát, vagyis $u$-t ekkor viszont $S$-nek kell kiszámítania, és odaadnia $A$-nak. A módosított protokoll a következő. A titkos kulcs megszerzése $S$-től:

$$\begin{aligned} A \to S: &\quad v = \text{hash}(A) \\ S \to A: &\quad u \;\; (u^{-b} = v \pmod{n}) \end{aligned}$$

Az $A$ azonosítja magát $B$-nek:

$$\begin{aligned} A \to B: &\quad \gamma = k^b( \pmod{n}) \qquad k \text{ véletlen} \\ B \to A: &\quad r \\ A \to B: &\quad y = k{\cdot}u^r \pmod{n} \\ B: &\quad \gamma \stackrel{?}{=} y^b \cdot \text{hash}(A)^r \pmod{n} \end{aligned}$$