

[A] TIIVISTELMÄ - SAMMANDRAG



(11) (21) Patentihakemus - Patentansökan 940364

(51) Kv.1k.5 - Int.cl.5

H 04L 9/32

S U O M I - F I N L A N D

(FI)

Patentti- ja rekisterihallitus  
Patent- och registerstyrelsen

(22) Hakemispäivä - Ansökningsdag	25.01.94
(24) Alkupäivä - Löpdag	24.07.92
(41) Tullut julkiseksi - Blivit offentlig	25.01.94
(86) Kv. hakemus - Int. ansökan	PCT/US92/06184
(32) (33) (31) Etuoikeus - Prioritet	
26.07.91 US 736451 P	

(71) Hakija - Sökande

1. United States Government as Represented by the Secretary of Commerce National Institute of Standards and Technology, Physics Building, Room A358, Gaithersburg, Md. 20899, USA, (US)

(72) Keksijä - Uppfinnare

1. Kravitz, David William, 12048 Long Lake Drive, Owings Mills, Md. 21117, USA, (US)

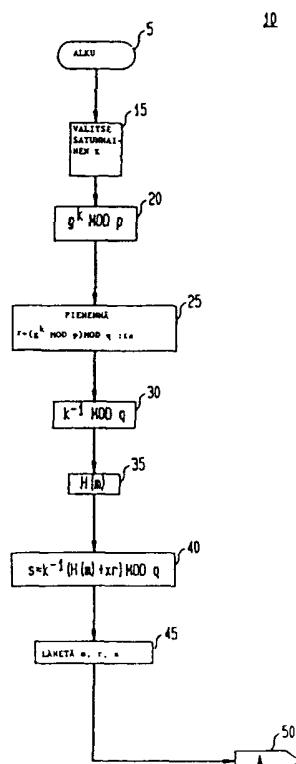
(74) Asiamies - Ombud: Oy Kolster Ab

(54) Keksinnön nimitys - Uppfinningens benämning

Digitaalinen allekirjoitusalgoritmi  
Digital signaturalgoritm

(57) Tiivistelmä - Sammandrag

Keksintö koskee menetelmää, jolla synnytetään ja vahvistetaan sanoman digitaalinen allekirjoitus. Tämä menetelmä edellyttää vastaanavien julkisen ja salaisen avaimen ( $y$  ja  $x$ ) parin kullekin allekirjoittajalle sekä julkisen ja salaisen arvon ( $r$  ja  $k$ ) parin, jotka synnytetään kullekin tämän allekirjoittajan sanomalle. Julkinen arvo  $r$  lasketaan säännön  $r = (g^k \bmod p) \bmod q$  mukaan. Arvo  $s$  valitaan sitten säännön  $s = k^{-1}(H(m) + xr) \bmod q$  mukaan, missä  $H$  on tunnettu tavanomainen hajausfunktio. Sano-ma  $m$  lähetetään sitten yhdessä allekirjoituksen  $(r,s)$  kanssa. Kun lähetetty signaali vastaanotetaan, suoritetaan vahvistusprosessi. Vastaanotetut arvot  $r$  ja  $s$  testataan, jotta määritettäisiin, ovatko ne kongruenteja  $0 \bmod q$ . Tämän lisäksi testataan  $r$ , jotta määritettäisiin, onko se  $v \bmod q$ , missä  $v$  lasketaan  $r$ :stä,  $s$ :stä,  $m$ :stä ja  $y$ :stä. Laillisesti suoritetuille allekirjoituksille  $v = g^k \bmod p$ .



Uppfinningen avser ett förfarande för generering och verifikation av en digital underskrift för ett meddelande. Förfarandet förutsätter ett par av motsvarande offentliga och hemliga nycklar ( $y$  och  $x$ ) för varje undertecknare samt ett par av ett offentligt och ett hemligt värde ( $r$  och  $k$ ), som genereras för varje meddelande av undertecknaren. Det offentliga värdet  $r$  beräknas enligt regeln  $r = (g^k \bmod p) \bmod q$ . Ett värde  $s$  väljs sedan enligt regeln  $s = k^{-1}(H(m) + xr) \bmod q$ , vari  $H$  är en känd konventionell spridfunktion. Meddelandet  $m$  sänds därpå tillsammans med underskriften  $(r, s)$ . Då den sända signalen mottas utförs en verifikationsprocess. De mottagna värdena  $r$  och  $s$  testas för bestämning av huruvida de är kongruenta med  $0 \bmod q$ . Dessutom testas  $r$  för bestämning av huruvida det är lika med  $v \bmod q$ , vari  $v$  beräknas ur  $r$ ,  $s$ ,  $m$  och  $y$ . För legitimt utförda underskrifter är  $v = g^k \bmod p$ .