公開鍵･秘密鍵生成条件

$gcd(p-1, x)=1$

$gcd(p-1, k_2)=1,\ gcd(p-1, k_2-1)\neq 2$

【鍵生成】 大きな素数 p と、p を法とする乗法群の要素 x を選び、 $k_1=a^x \bmod p$

(a は p を法とする乗法群の原始根)を計算する。

【公開鍵】 $k_1,\ k_2,\ p,\ a$

【秘密鍵】 x

【署名生成】 送信者は乱数 r を生成し、以下の計算によって署名 $(s,\ t)$ を生成する。

ただし、平文を M、ハッシュ関数を h とする。

$$s=\frac{(r(1-k_2)+h(M))}{xk_2} \bmod (p-1)$$

$$t=a^r \bmod p$$

【署名検証】 受信者は、公開鍵 k_1 を利用して、以下の等式が成立するか否かを検証する。

$$a^{(h(M))} * a^r = ((k_1)^s * a^r)^{(k_2)} \bmod p$$

【偽造方法】

壱: r をでっち上げてから r に対応する s を求める場合。

$$k_1^s = a^{(h(M)+r(1-k_2))} \bmod p$$

右辺は計算できるので、右辺の値に対応する s を求めることになるが、

これは難しい。

弐: s をでっち上げてから s に対応する a^r を求める場合。

$$a^{(r(k_2-1))} = a^{(h(M)-xk_2 s)} \bmod p$$

右辺は計算できるので、右辺の値に対応する a^r を求めることになるが、

$gcd(p-1, k_2-1)\neq 1$ より、 a^r を求めることは困難だと思われる。

執筆者 梅どぶろく ◆21Da3ggG3M