Tutorial VII group 2

31 October 2019 16:07

DIGITAL SIGNATURES

↳ RSA signatures

↳ El Gamal signatures

↳ DSA

Sign message w

$Sig(w)$

$(w, Sig(w))$

1.) Everyone should be able to verify that the message was signed by the correct user → Public key

2.) Only the correct user can sign messages. → Private key

RSA signature

Elements: p, q large primes, $n = p \cdot q$, Euler's theta function

e, d : $e = d^{-1} \mod \varphi(n)$ $\varphi(n) = (p-1)(q-1)$

PRIVATE: d, (p, q)

PUBLIC: e, n

TO SIGN w: $Sig(w) = w^d \mod n$

To sign w: $Sig(w) = w^d \mod n$

To verify $(w, Sig(w))$: $(Sig(w))^e \stackrel{?}{=} w \mod n$

How to fake a signature?

1.) Factorize n
2.) Calculate $\varphi(n)$
3.) Invert e (RSA problem)
4.) $\underbrace{Sig(w) = w^d \mod n}_{\text{discrete logarithm}}$

All computationally hard

How to break a signature scheme

Existential forgery – There exists a message for which a signature can be calculated efficiently

Universal forgery – All messages can be signed by the adversary (efficiently)

RSA existential forgery

Valid pair (w, s)

Can you calculate other valid pairs?

(w^2, s^2) is a valid pair as well

(w^2, s^2) is a valid pair as well

$$Sig(w^2) = (w^2)^d = (w^d)^2 = Sig(w)^2 = s^2 \mod n$$

Hash functions

$h: I \longrightarrow K \qquad |I| \gg |K| \approx 320$ bits

Cryptographic hash function

1.) it is hard to invert h: given $k \in K$ it is (computationally) hard to find $i \in I$, s.t. $h(i) = k$

2.) it is hard to find collisions: it is (computationally) difficult to find $i_1, i_2 \in I$ s.t. $h(i_1) = h(i_2)$

$[w, h(w), Sig(h(w))]$

Advantage I: signature needs to be calculated only for a short message.

Advantage II: security! Invalidates existential forgeries

$[w, h(w), Sig(h(w))]$

$[w', h(w)^2, Sig(h(w))^2]$

The adversary needs to find w', s.t. $h(w') = \underline{h(w)^2}$

El Gamal Signatures

Elements:

p - large prime

q - a primitive element of $\mathbb{Z}_p^*$

x - secret exponent $1 < x < p-1$

$y = q^x \mod p$

Private: x

Public: p, q, y

To sign w:

1.) $r \in \mathbb{Z}_{p-1}^*$ ← multiplicative group mod $p-1$

multiplicative inverse a^{-1} exists iff $\gcd(a, p-1) = 1$

All numbers coprime to $p-1$

$(a.b)^{-1} = a^{-1}.b^{-1}$

2.) $a = q^r \mod p$

3.) $b = r^{-1} \cdot (w - a.x) \mod p-1$ ← inverse mod $p-1$

To verify $(w, (a,b))$

$$q^w \stackrel{?}{\equiv} y^a a^b \mod p$$

$$\equiv (q^x)^a (q^r)^b \mod p$$

$$\equiv q^{ax} q^{r \cdot (r^{-1} (w - ax))} \mod p$$

$$\boxed{a^{p-1} \equiv 1 \mod p}$$

$$\equiv g^{ax} \cdot g^{w} \cdot g^{-ax} \mod p$$

$$\equiv g^{w} \mod p$$

Vulnerabilities HW 2

a.) There is an existential forgery for El Gamal signatures (which does not need a valid pair $(w,(a,b))$)

b.) Given $(w,(a,b))$ it is possible to calculate signature of $w' = \alpha(w + \beta . b) \mod p-1$, where $h = g^{\beta} \mod p$

$\beta \in \mathbb{Z}_p^*$

$\boxed{c.)}$ Given $(w_1,(a,b_1))$ and $(w_2,(a,b_2))$ it is possible to calculate x and thus totally break the scheme.

How to solve:

this is not necessarily a prime

$ax \equiv b \mod n$?

1.) $\gcd(a,n)=1$, calculate $a^{-1} \mod n$ and multiply both sides with a^{-1}.

2.) $\gcd(a,n)=k \wedge k \nmid b$, Solution doesn't exist.

3.) $\gcd(a,n)=k \wedge k \mid b$, then there are k solutions.

3.) $\gcd(a,n)=k \wedge k \mid b$, then there are k solutions.

Algorithm:

Solve

$$\frac{a}{k}x \equiv \frac{b}{k} \mod \frac{n}{k} \qquad \gcd\left(\frac{a}{k}, \frac{n}{k}\right) = 1$$

Solution to A is s.

Solutions to $ax \equiv b \mod n$ are $s + i\frac{n}{k}$ for $i \in \{0,1,\dots,k-1\}$

Example

$10x \equiv 5 \mod 15 \qquad \gcd(10,15) = 5$

Solve

$2s \equiv 1 \mod 3$

$s = 2$

$x = 2 + i \cdot 3 \quad i \in \{0,1,2,3,4\}$

$x \in \{2, 5, 8, 11, 14\}$

DSA - digital signature algorithm

Why is El gamal computationally inefficient?

1.) Size of signatures: $a \mod p \qquad \log_2 p$ bits

$b \mod p-1 \qquad \log_2 p$ bits

2.) both a, b are exponents in verification

Elements p - large prime ℓ-bit $(512 \le \ell \le 1024)$ $\ell = 64k$

q - 160-bit prime dividing $(p-1)$

$r = h^{\frac{(p-1)}{q}} \bmod p$, h is a primitive element of $\mathbb{Z}_p^*$

$$\{h, h^2, \ldots, h^{p-1}\} = \{1, \ldots, p-1\}$$

$\{r, r^2, \ldots, r^q\}$ Order of r in $\mathbb{Z}_p^*$ is q

$$(r^q) = \left(h^{\frac{(p-1)}{q}}\right)^q = h^{p-1} = 1 \bmod p \quad (\text{by FLT})$$

$$r^k \equiv r^{k \bmod q} \bmod p$$

$$\overbrace{\underbrace{r\,r\,r \cdots}_{\substack{q \\ \shortparallel \\ 1}} \underbrace{\quad \cdots \quad}_{\substack{q \\ \shortparallel \\ 1}} \underbrace{\quad\quad r}_{k \bmod q}}^{k}$$

PRIVATE: $1 < x < q$

PUBLIC: $p, q, r, y = r^x \bmod p$

SIGNATURE OF W: 1. Choose random $k \in \mathbb{Z}_q^*$

$$a = (r^k \bmod p) \bmod q$$

$a = (r \bmod p) \bmod q$

$b = k^{-1} \cdot (w + a \cdot x) \mod q$

k^{-1} inverse mod q

Verification: (of $(w, (a,b))$)

1.) $z \equiv b^{-1} \mod q$

2.) $u_1 \equiv w \cdot z \mod q$

3.) $u_2 \equiv a \cdot z \mod q$

$$(r^{u_1} \cdot g^{u_2} \bmod p) \bmod q \overset{?}{\equiv} a$$

$$(r^{w \cdot z} \cdot (r^x)^{a \cdot z} \bmod p) \bmod q \qquad b^{-1} \equiv k \cdot (w + ax)^{-1} \mod q$$

$$(r^{z(w+ax)} \bmod p) \bmod q$$

$$(r^{k \cdot (w+ax)^{-1} \cdot (w+ax)} \bmod p) \bmod q$$

$$(r^k \equiv a \bmod p) \bmod q$$

SUBLIMINAL CHANNELS

Note that ElGamal (DSA, OSS) use two secret numbers to sign w: random r

private x

to sign w: random r
private x

if x is shared between two parties r can be used to send secret messages.

$$b = r^{-1}(w - ax) \mod p-1$$

$$b \equiv x a \mod n$$

$\gcd(w-ax, p-1) = \xi$ does ξ divide b? YES

the correct r fullfills $a = g^r \mod p$