Signature Schemes

Signing Algo — Verification Algo

Sig_K (private) — x Message — Ver_K (public)

depends on a private key K

— Given a pair (x, y) → message, → singnature on x

$$Ver_K(x,y) \begin{cases} T & y = sig_K(x) \\ F & y \neq sig_K(x) \end{cases}$$

$\boxed{\text{Signature scheme}}$ (P, A, K, S, V) 5-tuple

$P \to$ $<\infty$ set of possible <u>messages</u>

$A \to$ $<\infty$ set of possible <u>signatures</u>

$K \to$ (<u>key space</u>) $<\infty$ set of possible <u>keys</u>

$\forall K \in K$, there is a signing algo $sig_K \in S$
and a corresponding verification algo $ver_K \in V$.

(sometime ↓ is randomized)
$Sig_K : P \to A$ s.t.

<u>fns.</u> $ver_K : P \times A \to \{true, false\}$
(poly. time fns) $\forall x \in P$ and $\forall$ signature $y \in A$

$$ver_K(x,y) = \begin{cases} true & \text{if } y = sig_K(x) \\ false & \text{if } y \neq sig_K(x) \end{cases}$$

— A pair (x,y) with $x \in P$ and $y \in A$ is called a <u>signed message</u>.

- Given a message x, it shd. be computationally infeasible for anyone (except Alice) to compute a signature y s.t. $ver_K(x,y) = T$
  (there might be >1 such y for a given x)
  depends upon how $ver_K(x,y)$ is defined)

- If Oscar can compute a pair (x, y) s.t. $ver_K(x,y) = T$ and x was not previously signed by Alice, then the signature y is called a <u>forgery</u>.

$$\boxed{\text{RSA Signature Scheme}}$$

$n = pq$ (p, q are primes)

$P = A = \mathbb{Z}_n$ define

$K = \{(n, p, q, a, b) : n = pq,\ ab \equiv 1 \pmod{\phi(n)}\}$

- The values n & b $\rightarrow$ public key
- p, q & a are private key
- For $K = (n, p, q, a, b)$ define

$$sig_K(x) = x^a \pmod n$$

and $ver_K(x, y) = T$ iff $x \equiv y^b \pmod n$
for $x, y \in \mathbb{Z}_n$

Note: ① Alice signs a message x using RSA decryption rule d_K. Alice (only person) can create the signature $\because d_K = sig_K$ is private
② The verification algo uses the RSA encryption rule e_K.
③ Any one can verify a signature $\because e_K$ is public.

Remark Anyone can forge Alice's RSA signature by choosing a random y and computing $x = e_K(y)$ then $y = sig_K(x)$ is a valid signature on the message x.
If this can be done then RSA signature scheme would be insecure.

forging can be eliminated

(1) Message contains suff. redundancy that a forged signature of this type does not correspond to a "meaningful" message x except with a very small prob.

(2) Use hash fn. + signature scheme

SECURITY REQUIREMENTS FOR SIGNATURE SCHEMES

ATTACK MODELS

(1) Key-only attack:
Oscar possesses Alice's public key i.e. the verification fn, ver_K.

(2) Known message attack:
Oscar possesses a list of messages previously signed by Alice, say
$(x_1, y_1), (x_2, y_2) \dots$

x_i: messages
y_i: Alice's sign on these (so $y_i = sig_K(x_i)$, $i = 1, 2, \dots$)

③ chosen message attack

Oscar ~~requires~~ requests Alice's signatures on a list of messages.

∴ He chooses $x_1, x_2, \ldots$

& Alice supplies her signatures on these

$$y_i = sig_K(x_i) \quad i = 1, 2, \ldots$$

ADVERSARIAL GOALS

Total Break Oscar determine Alice's private key i.e, sig_K

Selective forgery With some non-negligiable prob. Oscar is able to create a valid sign on a message chosen by some one else.

⇒ If Oscar is given a message x he can determine (with some prob.) a sign y s.t. $ver_K(x, y) = T$.

Existential forgery

Able to create a valid sign for >1 message.

create a pair (x, y) s.t. $ver_K(x, y) = T$.

SIGNATURES AND HASH FUNCTIONS

- The hash fn. $h : \{0,1\}^* \to Z$ Input message of arb. length
  Output MD of size (224 bits)
  MD is signed using signature scheme (P, A, K, S, V)
  where $Z \subseteq P$

message $\quad x \quad x \in \{0,1\}^*$

MD $\quad z = h(x) \quad z \in Z$

signature $\quad y = sig_K(z)$, $y \in Y$

$(x, y) \longrightarrow$ transmit

$\boxed{\text{Attack (1)}}$ Start with a valid signed message (x, y)
$y = sig_K(h(x))$

Compute $z = h(x)$ and attempts to find $x' \neq x$
s.t. $h(x') = h(x)$ if Oscar can do this
$\Rightarrow (x', y)$ valid signed message.
i.e. y is a forged signature for the message x'.
(Existential forgery)

$\boxed{\text{Attack (2)}}$ Oscar finds two messages $x \neq x'$
s.t. $h(x) = h(x')$

ElGamal Signature Scheme

- p prime s.t. dis. log prob. in $\mathbb{Z}_p$ is interactable
- $\alpha \in \mathbb{Z}_p^*$ a p.e.

Let $P = \mathbb{Z}_p^*$, $A = \mathbb{Z}_p^* \times \mathbb{Z}_{p-1}$

$K = \{(p, \alpha, a, \beta) : \beta \equiv \alpha^a \pmod p\}$

- p, α & β public key
- a private key

For $K = (p, \alpha, a, \beta)$ & for a (secret)

random no. $k \in \mathbb{Z}_{p-1}^*$

$$sig_K(x, k) = (r, \delta)$$

$$r = \alpha^k \bmod p$$

$$\& \quad \delta = (x - ar)k^{-1} \bmod (p-1)$$

For $x, r \in \mathbb{Z}_p^*$ & $\delta \in \mathbb{Z}_{p-1}$

$$ver_K(x, (r, \delta)) = T \Leftrightarrow \beta^r r^\delta \equiv \alpha^x \pmod p$$

$$\beta^{r} r^{\delta} \equiv \alpha^{ar} \alpha^{k\delta} \equiv \alpha^{x} \pmod{p}$$

$$\therefore \; ar + k\delta \equiv x \pmod{p-1}$$

$$\Rightarrow \alpha^{x} \equiv \beta^{r} r^{\delta} \bmod p$$

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

$$\& \; \beta = \alpha^{a} \bmod p$$

$$\Rightarrow \alpha^{x} \equiv \alpha^{ar+k\delta} \bmod p$$

$\because$ α is p.e. mod p

$$\Leftrightarrow \; x \equiv ar + k\delta \pmod{p-1}$$

$\boxed{\text{Example}}$ $p = 467$ $\alpha = 2$, $a = 127$

$$\beta = \alpha^{a} \bmod p = 2^{127} \bmod 467$$
$$= 132$$

Alice want to sign $x = 100$ & she chooses a random no. $k = 213$ (note $\gcd(213, 466) = 1$ & $213^{-1} \bmod 466 = 431$)

$$\rightarrow r = 2^{213} \bmod 467 = 29$$

$$\& \; \delta = (100 - 127 \times 29)\, 431 \bmod 466 = 51$$

Anyone can verify the sign $(29, 51)$

$$\because \; 132^{29} \cdot 29^{51} \equiv 189 \bmod (467)$$

$$\& \; 2^{100} \equiv 189 \pmod{467}$$

$\therefore$ sign is valid.

$\boxed{\text{Quiz}}$ E.C. over $GF(5^2)$ elements

x^2+4x+2 irr. poly over $GF(5) = \mathbb{Z}_5$

$$\mathbb{Z}_5[x]/(x^2+4x+2) = GF(25) = \mathbb{F}_{25}$$

let $E: y^2 = x^3+x+4$ over $\mathbb{F}_{25}$

Find all points on the E.C. over $\mathbb{F}_{25}$.

~~$GF(25) = \{0,1,2,3,4,\omega,\omega+1$~~

$GF(25) = \{0,1,2,3,4,\alpha,\alpha+1,\alpha+2,\alpha+3,\alpha+4,$
$2\alpha, 2\alpha+1, 2\alpha+2, 2\alpha+3, 2\alpha+4,$
$3\alpha, 3\alpha+1, 3\alpha+2, 3\alpha+3, 3\alpha+4,$
$4\alpha, 4\alpha+1, 4\alpha+2, 4\alpha+3, 4\alpha+4\}$