FORMULARIO CRYPTO V3

GALOIS LFSR

$$\begin{cases} s' = \text{shiftR}(s) & s_{m-1} = 0 \\ s' = SR(s) + P & s_{m-1} = 1 \end{cases}$$

OR

$$s' = x \cdot s \rightarrow s' = s' \cdot \frac{1}{P}$$

FIBONACCI LFSR

$$s_2 = \sum_{0}^{n-1} s_i p_j$$

$$s_3 = \sum_{0}^{n-1} s_{i+1} p_j$$

$$\vdots$$

if p all 1s $\Rightarrow$ max len $(2^m - 1)$

LINEAR PRNG

$$s_0 = \text{seed}$$

$$s_{i+1} = a s_i + b \bmod m$$

GAUSS JORDAN

$a^{-1} \bmod m$

linear ops.

$$\left(\begin{array}{c|c} a & 1 \\ m & 0 \end{array}\right) \rightarrow \left(\begin{array}{c|c} 1 & \\ c & a^{-1} \end{array}\right)$$

MULTIPLICATIVE INVERSE

existence: $\gcd(a, m) = 1$

CHINESE REMAINDER THEOREM

$$f(a,b) = a f(1,0) + b f(0,1)$$

$$f(1,0) = \begin{cases} y = 1 \\ y = 0 \end{cases} \dots$$

QUADRATIC RESIDUES EULER'S CRITERION

$$r^{\frac{p-1}{2}} \equiv \begin{cases} 1 \bmod p & \text{if } \exists r \in \mathbb{Z} \mid r = x^2 \bmod p \\ -1 \bmod p & \text{if } \nexists \end{cases}$$

p prime, r coprime

QUADRATIC RESIDUES GENERAL APPROACH

$x^2 \equiv r \bmod n$

- $r=0 \rightarrow$ 1 sol $x \equiv 0 \bmod n$
- $r>0 \rightarrow x^2 \equiv a \bmod p^k$
  - p odd $\rightarrow$ euler $\begin{cases} a^{\frac{p-1}{2}} = 1 \text{ 2 sols} \\ -1 \text{ no sol} \end{cases}$
  - $p=2$
    - $k=1$ 1 sol $x \equiv 1 \bmod 2$
    - $k=2$ 2 sol $x \equiv 1 \bmod 4, x \equiv 3 \bmod 4$ (only if $a \equiv 1 \bmod 4$)
    - $k=3$ 4 sol $\{1,3,5,7\}$ if $a \equiv 1 \bmod 8 (2^k)$
    - ⋮

EULER'S PHI

$\Phi = \prod (p_i^{e_i} - p_i^{e_i - 1})$ ← no. integers coprime to m in $\mathbb{Z}_m$

FERMAT'S LITTLE THEOREM

$a^p \equiv a \bmod p$ p prime

EULER'S THEOREM

$a^{\Phi(m)} \equiv 1 \bmod m$

RSA CRYPTOSYS.

$PK = (n, e)$ $y = x^e \bmod n$

$SK = (d)$ $x = y^d \bmod n$

Keygen

- $n = pq$
- $\phi(n) = (p-1)(q-1)$
- $e \in \{1, 2, \ldots, \phi(n)-1\} \mid \gcd(e, \phi(n)) = 1$ → 3, 17, 65537 are FAST!
- $d \cdot e \equiv 1 \bmod \phi(n)$ ← use eea

S-A-M ALGO. FAST EXPONENT

$$X^n \rightarrow BIN(n) \rightarrow \begin{cases} 1 = SQ \text{ and } MUL \\ 0 = SQ \end{cases}$$

(SCAN from MSB)

RSA-CRT APPROACH

$$y_p = y \bmod p$$
$$y_q = y \bmod q$$
$$d_p = d \bmod p$$
$$d_q = d \bmod q$$
$$x_p = y_p^{d_p} \bmod p$$
$$x_q = y_q^{d_q} \bmod q$$

$$X \equiv [qc_p]x_p + [pc_q]x_q \bmod n$$
$$c_p = q^{-1} \bmod n$$
$$c_q = p^{-1} \bmod q$$

D-H KEY EXCHANGE

p large prime, $\alpha \in \{2 .. p-2\}$ } public params.

(α: generator)

$$K_{pr} = a \in \{2 .. p-2\}$$
$$K_{pub} = A = \alpha^a \bmod p$$
$$K_{AB} = B^a \bmod p$$

ELGAMAL ENCRYPTION

p large prime, α generator } public

$$K_{pr} = i \in \{2, \ldots, p-2\}$$
$$K_E = K_{pub} = \alpha^i \bmod p$$

} change every message!

joint key:

$$K_H = B^i \bmod p$$

enc: $x \in \mathbb{Z}_p^*$, $y = x \cdot K_M \bmod p$

dec: $x \equiv y \cdot K_M^{-1} \bmod p$

GROUPS $|\mathbb{Z}_n^*| = \phi(n)$ ← euler's phi $\prod(p^{e_i} - p^{e_i - 1})$

$|\mathbb{Z}_n| = n+1$??

$\text{ord}(\alpha) = |G|$ ← generator

$|\mathbb{Z}_n^*| = \phi(n)$. $g^{|G|} = 1 \quad \forall a \in G$

. ord(a) divides $|G|$, ord(a) is lowest s.t. $a^e \equiv 1 \% n$

. no.generators $= \phi(|G|)$

. $\forall a \in G \mid \text{ord}(a) = s$ generates a cyclic s.group with $|H| = s$

Lagrange Theorem → . $|H|$ divides $|G|$, H s.group of G

DSA

KEY GEN

- p — 1024 bit prime
- q — 160 bit divisor of $p-1$
- α — s.t. $\text{ord}(\alpha) = q$
- d — s.t $0 < d < q$
- $\beta = \alpha^d \bmod p$

SIG GEN

- K_E — $0 < K_E < q$
- $r \equiv (\alpha^{K_E} \bmod p) \bmod q$
- $S \equiv (SHA(x) + dr) K_E^{-1} \bmod q$

$PK = (p, q, \alpha, \beta)$

$Sk = d$

SIG VERIFY

$w = s^{-1} \bmod q$

$u_1 = w \cdot SHA(x) \bmod q$

$u_2 = w \cdot r \bmod q$

$v \equiv (\alpha^{u_1} \beta^{u_2} \bmod p) \bmod q$

if $v \equiv r \bmod q \Rightarrow$ SIG OK!

ECC

$P + \Theta = P \qquad -P = (x_P; -y_P) \bmod n$

$P + (-P) = \Theta$

- Point addition

$x_3 = s^2 - x_1 - x_2 \bmod p$

$y_3 = s(x_1 - x_3) - y_1 \bmod p$

$$s = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} \bmod p & \text{if } P_1 \neq P_2 \\ \frac{3x_1^2 + a}{2y_1} \bmod p & \text{if } P_1 = P_2 \end{cases}$$

← from curve

- D-A-Add

$$\begin{cases} 1 & 2res_i + P \\ 0 & 2res_i \end{cases}$$

$res_0 = 2\Theta + P = P$

ECDH

p prime
$E: y^2 \equiv x^3 + ax + b \mod p$
$P = (x_P, y_P)$

} domain

$K_{prA} = a \in \{2, 3 \dots \#E - 1\}$ ← no. points in the curve

$K_{pubA} = aP = A$

$T_{AB} = bA$

ECDSA

KEY GEN

- P
- a, b curve coeff.
- A point, gen. ord $= q$
- d s.t $0 < d < q$ ← private
- $B = dA$

SIG GEN

- K_E s.t. $0 < K_E < q$
- $R = K_E A$
- $r = x_R$ ← x coord. of R
- $s \equiv (h(x) + dr) K_E^{-1} \mod q$

$Pk = (p, a, b, q, A, B)$

$Sk = d$

SIG VER

- $w = s^{-1} \mod q$
- $u_1 = w h(x) \mod q$
- $u_2 = wr \mod q$
- $P = u_1 A + u_2 B$

if $x_P \equiv r \mod q \Rightarrow$ ver OK!

PROBABILI ESAME !

SALSA 20 QUARTERROUND

$$b = b \text{ XOR } [(a+d) \lll 7]$$
$$c = c \text{ XOR } [(b+a) \lll 9]$$
$$d = d \text{ XOR } [(c+b) \lll 13]$$
$$a = a \text{ XOR } [(d+c) \lll 18]$$

} 32-bit words

Blum Blum Shub PRNG

$$x_{i+1} \equiv x_i^2 \bmod N \leftarrow N = p \cdot q \text{ where } p,q \equiv 3 \bmod 4$$

bit

↳ $b_i = \text{parity}(x_i)$

↑ LSB(even:0, odd:1)

BIRTHDAY ATTACK

$$N = 2^{\frac{n+1}{2}} \cdot \sqrt{\log_n\left(\frac{1}{1-\lambda_N}\right)}$$

RABIN CRYPTOSYS

$Pk = N \quad N = pq$

$SK = (p,q)$

enc: $C = m^2 \bmod N$

dec: $m_p = C^{\frac{p+1}{4}} \bmod p \quad m_q = C^{\frac{p+1}{4}} \bmod q$

4 candidates are generated !

LAMPORT-DIFFIE

$m' = m \| \text{NOT } m$

- MERKLE

$m' = m \| \text{1s of NOT } m$ ← len = $\log_2 n$ (bits of m)

SCHNORR SIGNATURE (based on FIAT-SHAMIR)

SK: x

PK: (g, y) where $y = g^x$

$r = g^k$ k random $\quad e = H(r \| M)$

$s = k - xe$

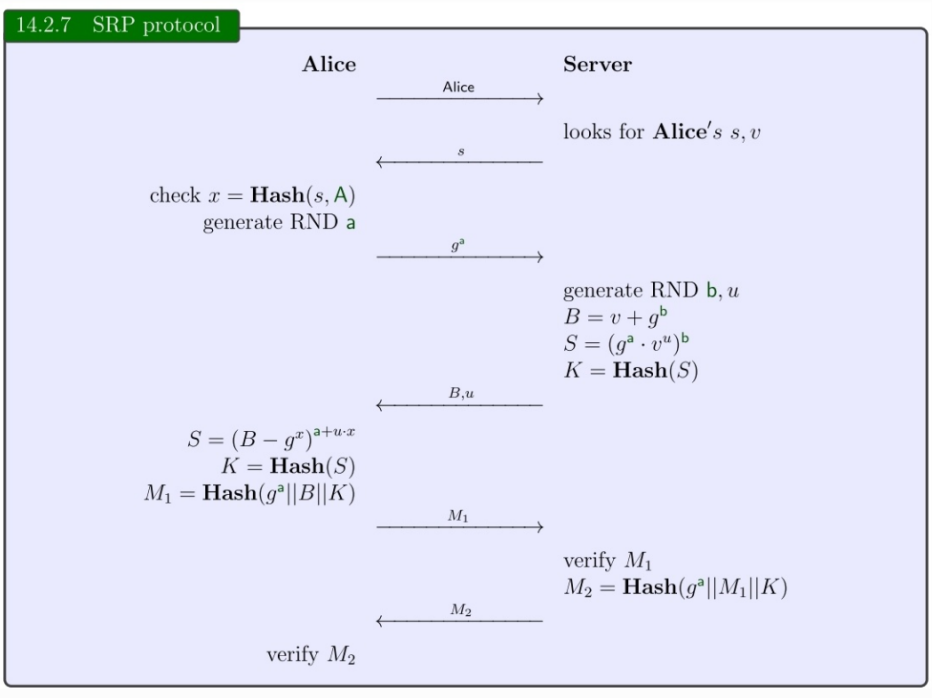
Sig: (s, e) ver: $r_v = g^s y^e$

$e_v = H(r_v \| M)$

OK if $e_v = e$

SRP

14.2.7 SRP protocol



A = pwd

EC POINTS LINE?