Lehmer generator and LCG

$S_0 = \text{seed}$

$S_{i+1} \equiv aS_i + b \bmod m$

Fibonacci LFSR

$$P(x) = 1 + p_{m-1}x + \dots + p_1 x^{m-1} + p_0 x^m$$

$$\chi_L(x) = x^m P\left(\frac{1}{x}\right) = p_0 + p_1 x + \dots + p_{m-1}x^{m-1} + x^m$$

$$L = \begin{bmatrix} p_{m-1} & 1 & 0 & 0 \dots & 0 \\ p_{m-2} & 0 & 1 & 0 \dots & 0 \\ \vdots & & & & \vdots \\ p_1 & 0 & 0 & 0 \dots & 1 \\ p_0 & 0 \dots & & & 0 \end{bmatrix} \quad S = [S_{m-1} S_{m-2} \dots S_1 S_0]$$

$S \cdot L = S'$

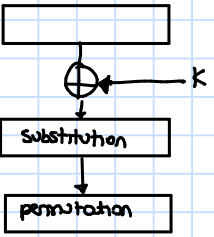
Galois LFSR

$$G(x) = \chi_L(x) = x^m + p_{m-1}x^{m-1} + \dots + p_1 x + p_0$$

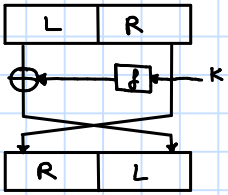
$$L = \begin{bmatrix} 0 & 1 & 0 \dots & 0 \\ 0 & 0 & 1 \dots & 0 \\ \vdots & & & \\ 0 & 0 & 0 \dots & 1 \\ p_0 & p_1 & p_2 \dots & p_{m-1} \end{bmatrix} \quad S = [g_0 g_1 \cdots g_{m-2} g_{m-1}]$$

$$S \cdot L = \begin{cases} \text{shiftright}(s) & \text{if } g_{m-1} = 0 \\ \text{shiftright}(s) \oplus p & \text{if } g_{m-1} = 1 \end{cases}$$

Substitution-permutation



Feistel network



RSA

- choose p, q, $N = pq$ and $\varphi(N) = (p-1)(q-1)$. Pick $e \in \mathbb{Z}^*_{\varphi(N)}$ compute $d = e^{-1} \bmod \varphi(N)$
- $sk = (\varphi(N), d)$, $pk = (N, e)$
- $Enc_{pk}(m)$ with $m \in \mathbb{Z}_N$; $C = m^e \bmod N$
- $Dec_{sk}(m) \Rightarrow m = C^d \bmod N$

DSA Key generation

- Generate a prime p
- find prime divisor q of $p-1$
- find an element $\alpha \in \mathbb{Z}_p$ with $\text{ord}(\alpha) = q$, i.e α generates the subgroup with q elements
- Choose rnd $d < q$
- compute $\beta = \alpha^d \bmod p$
- $pk = (p, q, \alpha, \beta)$

CBC Ciphering

$y_1 = Enc_K(B_1 \oplus IV)$

If $j > 1$ then $y_j = Enc_K(B_j \oplus y_{j-1})$

CBC Deciphering

$B_1 = Dec_K(y_1) \oplus IV$

If $j > 1$ then $B_j = Dec_K(y_j) \oplus y_{j-1}$

GCM Tag T

$H = Enc_K(0)$

$g_0 = AAD \otimes H$

$g_j = (g_{j-1} \oplus C_j) \otimes H$ for $j = 1, \dots, N$

$T = (g_N \otimes H) \oplus Enc_K(T_0)$

Euler's criterion

$r^{\frac{p-1}{2}} \equiv 1 \bmod p \Rightarrow$ quadratic residue

Euler's function

Given N = product of n prime factors p_i

$$\Phi(N) = \prod_{i=1}^{n} \left(p_i^{e_i} - p_i^{e_{i-1}}\right)$$

If $N = pq \Rightarrow \Phi(N) = (p-1)(q-1)$

Fermat little theorem

$r^p = r \bmod p$ with p prime

EC : point addition

$y^2 \equiv x^3 + ax + b \bmod p$

$P + Q = R$

$$\lambda = \frac{3x_1^2 + a}{2y_1} \text{ if } P = Q \qquad \lambda = \frac{y_2 - y_1}{x_2 - x_1} \text{ if } P \neq Q$$

$$\nu = y_1 - \lambda x_1$$

$$x_3 = \lambda^2 - x_1 - x_2 \qquad y_3 = -(\lambda x_3 + \nu)$$

DSA Signature

- Choose an integer as rnd ephemeral key $k_E < q$
- Compute $r \equiv (\alpha^{k_E} \bmod p) \bmod q$
- Compute $s \equiv (SHA(x) + d \cdot r) \cdot k_E^{-1} \bmod q$

$sig = (r, s)$

DSA verify

- compute auxiliary value $w = s^{-1} \bmod q$
- compute auxiliary value $u_1 \equiv w \cdot SHA(x) \bmod q$
- compute auxiliary value $u_2 \equiv w \cdot r \bmod q$
- compute $v \equiv (\alpha^{u_1} \cdot \beta^{u_2} \bmod p) \bmod q$

If $v == r$ VALID

ElGamal encryption

Parameter domains: g and p as in DH

- $Gen(\lambda)$: pick $A \in \{1, \dots, p-1\}$ and compute $h = g^A = g^{SK}$. Set $pk = h$
- $Enc_{PK}(m)$ with $m \in GF(p)$: pick RND $B \in \{1, \dots, p-1\}$ and compute $C = (g^B, m \cdot h^B)$
- $Dec_{SK}(C)$ with $C = (c_1, c_2)$; compute $m = c_2 / c_1^A$

Rabin

- $Gen(\lambda)$: choose $p, q \equiv 3 \bmod 4$ (prime numbers of λ bit), compute $N = pq$
- set $pk = N$, $SK = (p, q)$
- $Enc_{PK}(m)$ with $m \in \mathbb{Z}_N$; compute $C = m^2 \bmod N$
- $Dec_{SK}(C)$: compute $m_p = C^{\frac{p+1}{4}} \bmod p$, $m_q = C^{\frac{p+1}{4}} \bmod q$
  CRT gives four candidates for m: $(\pm m_p, \pm m_q)$

ECDSA Sign

Choose RND $K_E < n$

$R = K \cdot G = (x_R, y_R)$, Set $r = x_R$

$s = (hash(M) + d \cdot r) K_E^{-1} \bmod n$. If $s = 0$

$Sign(M) = (r, s)$

ECDSA verify

$w = s^{-1} \bmod n$; $u_1 = w \cdot hash(M) \bmod n$

$u_2 = w \cdot r \bmod n$; $P = u_1 \cdot G + u_2 \cdot B = (x_P, y_P)$

If $x_P == r \bmod n$

EC DH

Alice & Bob agree on E and a point $G \in E$

They choose A, B (sk) and compute $pk_A = A \cdot G$; $pk_B = B \cdot G \Rightarrow$ exchange

Session Key $K_{AB} = A \cdot pk_B = B \cdot pk_A$

EC-Massey-Omura

Alice has a secret key $0 < A < n$ s.t. $gcd(A, n) = 1$, Bob has B

Alice		Bob
$C_0 = A \cdot M$	$\xrightarrow{C_0}$	
		$C_1 = B \cdot C_0$
	$\xleftarrow{C_1}$	
$C_2 = A^{-1} C_1$	$\xrightarrow{C_2}$	
		$M = B^{-1} C_2$

ECDSA

$sk = d$ rnd $\in \{1, \dots, n-1\}$

$pk = (p, a, b, n, G, B)$ where $B = d \cdot G$