Srovnání algoritmů DSA a ECDSA

DSA – Digital Signature Algorithm

- algoritmus pro digitální podpis
- velmi podobný El-Gamalovu podpisovému schématu

ECDSA - Elliptic Curve Digital Signature Algorithm

- algoritmus analogický s **DSA**
- místo operací v podgrupě řádu **q**, pracujeme s grupou na eliptické křivce nad polem $\mathbf{F_P}$.
- ECDSA je standardizovaný v **ANSI X.9F1** a **IEEE P1363**

DSA

1. Generování DSA klíče – první fáze

Každý účastník komunikace provede následující kroky:

1. Vybere prvočíslo q stejné délky, jako je požadovaná délka výstupu.
2. Vybere prvočíslo p délky L takové, že $p-1$ je násobek q.
3. Najde generátor g grupy F_p
4. Parametry systému jsou dány trojicí (p, q, g).

2. Generování DSA klíče – druhá fáze

1. Účastník vybere číslo **x** takové, že $0 < x < q$
2. Spočítá $y=g^x \bmod p$
3. Veřejný klíč je (p, q, g, y).
4. Soukromý klíč je x**.**

3. Generování podpisu pomocí DSA

Účastník A podepisující zprávu m provede následující kroky:

1. Vybere náhodné (a pro každou zprávu jedinečné) číslo k, takové, že $0 < k < q$
2. Spočítá $r = (g^k \bmod p) \bmod q$
3. Spočítá $s = (k^{-1}(H(m) + x*r)) \bmod q$, kde m zpráva a H je hashovací funkce
4. Pokud vyjde $s=0$ nebo $r=0$, vrátí se k bodu 1
5. Podpis je dvojice (r,s)

4. Ověření podpisu pomocí DSA

Účastník B ověřující zprávu m provede následující:

1. Pokud není splněna některá z podmínek $0< r <q$ nebo $0< s <q$, je zpráva odmítnuta.
2. Spočítá $w = (s)^{-1} \bmod q$
3. Spočítá $u_1 = (H(m)*w) \bmod q$
4. Spočítá $u_2 = (r*w) \bmod q$
5. Spočítá $v = ((g^{u1}*y^{u2}) \bmod p) \bmod q$
6. Podpis je platný, pokud $v = r$

ECDSA

Postup pro generování páru klíčů, generování podpisu a ověření podpisu ECDSA je následující.

1. Generování ECDSA klíče

Každý účastník A provede následující kroky:

5. Vybere eliptickou křivku E nad podložním polem F_P (p je prvočíslo).
6. Vybere bod P řádu n ležící na křivce E .
7. Vybere statisticky jedinečné a nepředvídatelné celé číslo d v intervalu $[1, n - 1]$.
8. Vypočte $Q = dP$.
9. Veřejný klíč je dán (E, P, n, Q). Soukromý klíč je d.

2. Generování podpisu ECDSA

Účastník A podepisující zprávu m provede následující kroky:

1. Vybere statisticky jedinečné a nepředvídatelné celé číslo k v intervalu $[1, n - 1]$.
2. Vypočte $kP = (x_1, y_1)$ a $r = x_1 \bmod n$. (kde x_1 je považován jako celé číslo, například převedené do binárního zápisu.).
   Jestliže $r = 0$, pak se vrátí ke kroku 1. (bezpečnostní podmínka: jestliže $r = 0$, pak podpisová rovnice $s = k^{-1}\{h(m) + dr\} \bmod n$ nezahrnuje soukromý klíč d!)
3. Vypočte $k^{-1} \bmod n$.
4. Vypočte $s = k^{-1}\{h(m) + dr\} \bmod n$,kde h je Secure Hash Algorithm (SHA-1).
5. Jestliže $s = 0$, pak se přejde znovu ke kroku 1. (Jestliže $s = 0$, pak $s^{-1} \bmod n$ neexistuje; s^{-1} je požadovaný v kroku 2 ověření podpisu.)
6. Podpis zprávy m je pár celých čísel (r, s).

3. Ověření podpisu ECDSA

Při ověření podpisu (dán dvojicí r, s), který vytvořil účastník A na zprávě m provede účastník B následující:

1. Obdrží autentickou kopii veřejného klíče (E, P, n, Q) od účastníka A. Ověří, že r a s jsou celá čísla v intervalu $[1, n - 1]$.
2. Vypočte $w = s^{-1} \bmod n$ a $h(m)$.
3. Vypočte $u_1 = h(m)w \bmod n$ a $u_2 = rw \bmod n$.
4. Vypočte $u_1P + u_2Q = (x_0, y_0)$ a $v = x_0 \bmod n$.
5. Akceptuje podpis pouze v případě, jestliže $v = r$.

Srovnání ECDSA a DSA

Shoda v zápisech výpočtů nad $E(F_P)$ a Z_P^*

Z historických důvodů se grupa operací pro eliptickou křivku nad $E(F_P)$ nazývá operací sčítání a grupa činností v Z_P^* se nazývá násobení. Rozdíly součtového zápisu a multiplikativní zápisu mohou být matoucí. Tabulka proto ukazuje shodu mezi zápisy užívanými pro obě grupy - Z_P^*a $E(F_P)$.

	Z_P^*	$E(F_p)$
Grupa		
Prvky grupy	celá čísla { 1, 2, . . ., p - 1 }	body (x,y) na E plus O „bod v nekonečnu“
Operace grupy	násobení modulo p	sčítání bodů
Zápis	Prvky: g, h Násobení: g • h Inverze: g^{-1} Dělení: g / h Umocňování: g^a	Prvky: P, Q Sčítání: P + Q Negace: -P Odčítání: P – Q Násobek: aP
Problém diskrétního logaritmu	Pro dané g $\in \mathbb{Z}_p^*$ a $h = g^a \bmod p$, cílem je nalézt a	Pro dané P $\in$ $E(F_p)$ a Q = aP, cílem je nalézt a.

Tabulka: Shoda mezi Z_P^* a $E(F_p)$ zápisem.

Rozdíly mezi ECDSA a DSA

Jediný významný rozdíl mezi ECDSA a DSA je v generování r. DSA vytváří tento náhodný prvek operací $(g^k \bmod p)$ a redukuje pomocí modulo q. Získává tak celé číslo v intervalu $[1, q - 1]$. ECDSA generuje celé číslo r v intervalu $[1, n- 1]$ na x-ových souřadnicích náhodného bodu kP a redukcí pomocí modulo n.
Podobnou úroveň bezpečí jako u DSA zajistíme (s 160bitovým q a 1024bitovým p**)**, parametr n by měl mít asi 160 bitů. Pro tento případ má pak DSA a ECDSA podpis stejnou bitovou délku (320 bitů).
Namísto generování vlastní eliptické křivky pro každého účastníka, mohou všichni účastníci užívat stejnou křivku E a bod P řádu n**.** V tomto případě závisí veřejný klíč pouze na bodu Q. Výsledkem jsou veřejné klíče menších velikostí.
Dále je možné provést kompresi souřadnic čímž lze bod $Q = (x_Q, y_Q)$ vyjádřit pomocí x-ové souřadnice x_Q a jednoho bitu y-souřadnice y_Q. (souřadnici y při znalosti souřadnice x a podložní křivky lze dopočítat, jeden bit souřadnice y určí její znaménko). Jestliže prvočíslo p má velikost 160 bitů (definující podložní pole F_P), pak veřejný klíč může být reprezentován 161 bitovým řetězcem.