Elliptical Curves in DNSSEC

Dmitry Kohmanyuk
Communication Systems Ltd
Kyiv, UAdom 2013

Elliptic Curve Cryptography (ECC)

- y^2 = x^3 + ax + b

http://en.wikipedia.org/wiki/Elliptic_curve

http://en.wikipedia.org/wiki/Elliptic_curve_cryptography

Digital Signature Algorithm (DSA)

- FIPS 186
- U.S. Patent 5,231,668 invented by David Kravitz (ex-NSA)
- owned by DoC, royalty-free by NIST
- http://en.wikipedia.org/wiki/Digital_Signature_Algorithm

ECDSA: DSA + ECC

- RFC 5114: Additional Diffie-Hellman Groups for Use with IETF Standards
- http://en.wikipedia.org/wiki/Elliptic_Curve_DSA
- FIPS 186-3

Benefits

- smaller public key: 80 bits secret, 160 bits ECDSA (1024 bits plain DSA)
- new mathematics (more secure?)
- randomness used

Issues

- more computational resources
- compatibility issues
- patents

- In 2013, the New York Times revealed that Dual Elliptic Curve Deterministic Random Bit Generation (or Dual_EC_DRBG) had been included as a NIST national standard due to the influence of NSA, which had included a deliberate weakness in the algorithm and the recommended elliptic curve. RSA Security in September 2013 issued an advisory recommending that its customers discontinue using any software based on Dual_EC_DRBG.[28] In the wake of the exposure of Dual_EC_DRBG as "an NSA undercover operation", cryptography experts have also expressed concern over the security of the NIST recommended elliptic curves, suggesting a return to encryption based on the discrete logarithms.[29]

Internet and ECC

- TLS (RFC 4492)
- IPsec IKE (RFC 4754)
- X.509 PKI (RFC 3279, 5480)
- XML (RFC 4050)
- DNSSEC (RFC 6944)

DNSSEC RFCs

- main - RFC 4033, 4034, 4035
- SHA-256 digest - RFC 4509
- NSEC3 - RFC 5155
- SHA-2 with RSA - RFC 5702 (used by UA, algorithm 10, RSA/SHA-512)
- Applicability statement for DNSSEC algorithms - RFC 6944

DNSSEC algorithms

- http://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xhtml
- RFC 6014: Cryptographic Algorithm Identifier Allocation for DNSSEC
- 12 | GOST R 34.10-200 | ECC-GOST | RFC 5933
- 13 | ECDSA Curve P-256 with SHA-256 | ECDSAP256SHA256 | RFC 6605
- 14 | ECDSA Curve P-384 with SHA-384 | ECDSAP384SHA384 | RFC 6605

Elliptic Curves in DNS

- RFC 5933: Use of GOST Signature Algorithms in DNSKEY and RRSIG Resource Records for DNSSEC
- RFC 6605: Elliptic Curve Digital Signature Algorithm (DSA) for DNSSEC
- RFC 5114: Additional Diffie-Hellman Groups for Use with IETF Standards

ECDSA: Recommended by RFC 6944

- «Likewise, ECDSA with the two identified curves (ECDSAP256SHA256 and ECDSAP384SHA384) is an algorithm that may see widespread use due to the perceived similar level of security offered with smaller key size compared to the key sizes of algorithms such as RSA. Therefore, ECDSAP256SHA256 and ECDSAP384SHA384 are Recommended to Implement.»

Let us try it!

- dk@cctld.ua
- www.hostmaster.ua/dnssec
- *dig +dnssec dnskey ua.*