MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Digital Signatures: DSA with Medium Fields

Author: Tanja Lange

July 2011

Discrete Logarithm Problem (DLP)

The term *Discrete Logarithm Problem (DLP)* refers to the problem of solving the equation

$$\alpha^x = \beta,$$

i. e., computing the *secret* integer x, where the base α is a fixed element of a finite group and β is chosen randomly in the subgroup $G = \langle\alpha\rangle$ generated by α.
The cryptographic strength of the NIST standard DSA [3] for digital signatures is related to the difficulty of DLP in a cyclic subgroup G of the multiplicative group L^* of a finite field L. Also in the ElGamal encryption the security depends on the intractability of the DLP.

To avoid attacks using the Chinese Remainder Theorem [4], one restricts the computation to a subgroup of prime order l. As the computations are done in a group, generic attacks like the Pollard rho method or Baby-Step-Giant-Step techniques can be applied; their running time is $O(\sqrt{l})$. For concrete instantiations of the group, other attacks might be feasible to mount, most prominently index calculus attacks.

For example if the group is a subgroup of the multiplicative group of a finite field L, index calculus attacks in the field can be used. Their complexity is subexponential in the size of the finite field. To balance the strengths of the attacks it is a common choice is to use a prime order subgroup of L^*; this is also suggested in the DSA standard.

In the original standard, L has characteristic 2. In contrast, our challenge concerns the case of "medium" fields, where $L = \mathsf{GF}(p^n)$ with a balanced relation between characteristic p and extension degree n.

There are several reasons for applying such fields if just a finite field is needed. Most prominently is the good performance of modular arithmetic if the modulus fits exactly in one word of the processor. In addition to this, one can use primes such that a sparse polynomial generates the extension field. In particular the binomial $x^n - 2$ is preferred due to its small absolute term. These ideas are used in *Optimal Extension Fields* [2] and *Processor Adapted Finite Fields* [1] and the cited papers report good timings for the finite field arithmetic.

For powers of very small primes and for large prime fields the function-field sieve and the number-field sieve are highly optimized; for intermediate fields algorithms with the same asymptotic behavior exist but the actual running times are slower.

Our challenge aims at encouraging research into the intermediate range. The parameters are chosen in a manner that the subgroup has very large order (380 bits), such that the generic square root attacks cannot be applied successfully, but the finite field itself has less than 550 bits. Therefore, we expect that a successful computation of the discrete logarithm in our challenge requires at least a new implementation, if not new ideas for index calculus attacks.

The Challenge

Consider the finite field $L = \mathsf{GF}(p^n)$ for $n = 17$ and $p = 4294939399$. Let ξ be a root of the binomial $x^{17} - 2$, which is irreducible over $\mathsf{GF}(p)$. We have

$$L = \mathsf{GF}(p)[\xi].$$

The challenge is to compute the discrete logarithm of β with respect the base α for the $\alpha, \beta \in L^*$ specified below.

In the concrete implementation in a DSA scheme this means that the private key, which is used for signing documents, could be recovered from the public key, which is used to verify the signature of a document.

Detailed Technical Specification

The prime p was chosen to be close to 2^{32}, namely $2^{32} - p = 27897$, to facilitate use of fast modular arithmetic like in Montgomery representation.
We have $p \equiv 1 \bmod 17$ such that the 17-th roots of unity are in $\mathrm{GF}(p)$. One easily checks that the binomial $x^{17} - 2$ is irreducible and can therefore in fact be used to construct the field extension.

The element $\alpha \in L = \mathrm{GF}(p)[\xi]$ is defined as

$$\begin{aligned}\alpha \quad = \quad & 3861058060\,\xi^{16} + 3564986786\,\xi^{15} + 1476915385\,\xi^{14} + 378294953\,\xi^{13} + \\ & 527539873\,\xi^{12} + 2565028647\,\xi^{11} + 3524396659\,\xi^{10} + 4208613634\,\xi^{9} + \\ & 2860013058\,\xi^{8} + 461970796\,\xi^{7} + 514597914\,\xi^{6} + 2797025912\,\xi^{5} + \\ & 3012586214\,\xi^{4} + 3353183518\,\xi^{3} + 2428759997\,\xi^{2} + 195705603\,\xi + \\ & 2298553666.\end{aligned}$$

The subgroup generated by α has the following 380 bit prime order

$$\begin{aligned} \ell \quad = \quad & 31942746002831900219259425725947140359969100706564301948609 \\ & 93636464196107336401578556887158853243993141257232706302 9. \end{aligned}$$

The complete factorization reads

$$|L^*| = 2 \cdot 3 \cdot 17^3 \cdot 19 \cdot 103 \cdot 130363 \cdot 93668369 \cdot 13044863892859 \cdot 1961650989234689 \cdot \ell.$$

The element β of $\langle\alpha\rangle$ is defined as

$$\begin{aligned} \beta \quad = \quad & 1853776844\xi^{16} + 2979288427\xi^{15} + 548791496\xi^{14} + 1098158376\xi^{13} + \\ & 2912162188\xi^{12} + 591706410\xi^{11} + 396109450\xi^{10} + 1162714473\xi^{9} + \\ & 2696515674\xi^{8} + 2661468235\xi^{7} + 1529382184\xi^{6} + 3787954269\xi^{5} + \\ & 1349496244\xi^{4} + 1154080109\xi^{3} + 532866501\xi^{2} + 1397637821\xi + \\ & 752038700. \end{aligned}$$

It equals α^x for some secret integer x. The challenge is to compute this secret key for the given α and β.

References

- [1] R. Avanzi, P. Mihăilescu, *Generic efficient arithmetic algorithms for PAFFs (Processor Adequate Finite Fields) and related algebraic structures*, SAC 2003, Lecture Notes in Computer Science, vol. 3006, Springer-Verlag, Berlin, 2004, pp. 320–334.

- [2] D. V. Bailey, C. Paar, *Optimal extension fields for fast arithmetic in public key algorithms*, Advances in Cryptology – Crypto '98, H. Krawczyk (ed.), Lecture Notes in Computer Sciene, vol. 1462, Springer-Verlag, Berlin, 1998, pp. 472-485.

- [3] DSA web site of NIST: `http://www.itl.nist.gov/fipspubs/fip186.htm`

- [4] S. Pohlig, M. Hellmann, *An improved algorithm for computing logarithms over GF*(p) *and its cryptographic significance*, IEEE Trans. Inform. Theory **IT-24** (), pp. 106–110.