ON THE FEASIBILITY OF COMPUTING DISCRETE LOGARITHMS USING ADLEMAN'S SUBEXPONENTIAL ALGORITHM.*

(Summary)

by

Tore Herlestam

Department of Computer Engineering
University of Lund
P O Box 725
S-220 07 LUND
SWEDEN

May 6, 1982

Abstract - Some public key distribution systems, based on the difficulties in computing logarithms modulo a large prime, have been alleged to be insecure because of a statement that any logarithm modulo a 200 bit prime can be computed within a reasonable time by means of a subexponential algorithm due to Adleman.

In this commentary said algorithm is examined from an algebraic and number-theoretical point of view. The scrutiny shows that the algebraic model for the algorithm contains several traps which seem to be hard to circumvent, and also, not least, that the presupposed abundance of so called round numbers will not be at hand in the computationally interesting cases.

Hence it is concluded that the algorithm cannot be a serious threat to the mentioned public key distribution systems.

---

* This research was supported in part by the Swedish Board for Research and Development under grant 81-3323 at the University of Lund.

THE ALGEBRAIC MODEL

In a proper sense, logarithms can only be defined over a cyclic group, such as the multiplicative group of positive real numbers or the multiplicative group of a finite field. Since the group of units in the residue class ring Z/nZ is not cyclic in general, we shall confine ourselves here to the case $GF(p)$.

When p is a (large) prime, an important step in the algorithm [1] is the following. Let $q_1, q_2, \ldots, q_r$ be the primes less than a certain bound y, much smaller than p. Under multiplication in $GF(p)$ the elements of the form $q_1^{e_1} q_2^{e_2} \ldots q_r^{e_r}$ span a subgroup in $GF(p)^*$, and the exponent modulus is $p-1$. This subgroup can therefore be regarded as a module over the ring $Z/(p-1)Z$, with multiplication in $GF(p)$ as vector addition and exponentiation as scalar multiplication. Now it is assumed in [1] that when a generates $GF(p)^*$, a set of spanning elements $a^{r_1}, a^{r_2}, \ldots, a^{r_z}$ can be found for the module M within an affordable time bound by guessing the exponents r_j and checking.

Whether said assumption may be regarded as realistic or not depends evidently heavily on the magnitude of z. It is easily seen that z has to be around $\pi(y)$, the number of primes $\leq y$. When $y=7.5\ 10^{15}$, a value conforming to the ideas in [1] for $p = 10^{100}$, we have $\pi(y) \cong 2\ 10^{14}$, which shows that this step in the algorithm may certainly not be trivial.

We remark here that if one should try to transfer the algorithm to the case $GF(2^p)$ (cf [2]), then the module M will be a vector space over $GF(2^p-1)$ for such p that 2^p-1 is prime, but the difficulties in creating a spanning set of moderate size will be essentially unchanged.

The next step in Adleman's algorithm consists in expressing an arbitrary element b of the module M by means of the spanning set,

$$b = a^{x_1 r_1 + x_2 r_2 + \ldots + x_z r_z}.$$

This is meant to be achieved using gaussian elimination. But the ring in which we are working contains lots of divisors of zero. In fact, more than half of the ring elements are divisors of zero, because p-1 is even. In [1] these difficulties are grossly underestimated in the statement that "no problems arise".

The final step in the algorithm consists of solving for b in

$$b^r = a^{x_1 r_1 + x_2 r_2 + \ldots + x_z r_z}.$$

Again the divisors of zero prevent us from using the ordinary solving method, since in more than half of all cases r does not possess a multiplicative inverse in $Z/(p-1)Z$. Presupposing $\gcd(r,p-1)=1$ does not seem to help very much, since it restrains r severely when we are seeking r such that b^r is y-smooth. Summing up, we find that the algebraic model for the Adleman algorithm contains several traps which seem to be very difficult to circumvent.

THE SUPPLY OF ROUND NUMBERS

Following Hardy's terminology [3], a number is called round if it is composed of only small prime factors. It has long been known ([3], p 358) that round numbers are very rare. This is not, however, in agreeement with the statement in [1] "that a disproportionately large portion of numbers not only have a small prime factor but are entirely composed of small prime factors."

Conforming to conventional notations in number theory we define $\Psi(x,y)$ as the number of positive integers $\leq x$ not containing any prime factor $> y$. In what follows we assume that $^2\log y = c\sqrt{^2\log x \; ^2\log^2\log x}$ as in [1], and take c=1 as is usually done in discussions concerning Adleman's algorithm. The numbers counted by $\Psi(x,y)$ are called y-smooth.

For large x several asymptotic results have been obtained by different researchers [4,5,6,7,8]. Thus we have asymptotic upper bounds as well as lower bounds on $\Psi(x,y)/x$. In the

range of interest here the following numerical values may be quoted, with due reservations for the influence by unspecified constants in the bounds.

$^2\log x$	200	256	332 ($x=10^{100}$)
$\log y$	11.77	13.62	15.88
$\log \pi(y)$	10.34	12.13	14.32
$\log \Psi(x,y)/x \geq$	-10.6	-16.4	-17.0
$<$	-1.85	-2.61	-3.57

According to the current opinion (cf [9], p 300-303) the lower bound expresses the asymptotic behavior of $\Psi(x,y)/x$. Thus it seems pretty hard to find any evidence that y-smooth numbers should be abundant enough for the purposes in the Adleman algorithm. For instance, when $p \cong 10^{100}$, the proportion of smooth numbers lies between 10^{-17} and $3\ 10^{-4}$, probably near the lower end, and yet we have to find about 10^{14} of them by guessing and checking.

The optimism in [1] is based on the conviction that round numbers as used in the Morrison-Brillhart factoring scheme [10] could do equally well for computing discrete logarithms. Unfortunately their role in the factoring method is quite different. Firstly, they do not need to be abundant in order that the Morrison-Brillhart technique shall work. Secondly, and most importantly, they are only used to create linear dependence over GF(2) in the factoring scheme, as opposed to achieving a generating set over $\mathbb{Z}/(p-1)\mathbb{Z}$ in the logarithm case.

Thus the analysis of the Morrison-Brillhart factoring method by Dixon [11] cannot be transferred to the logarithm procedure discussed here.

We conclude that it must be impossible to predict any success with Adleman's algorithm out from known running times for implementations of the Morrison-Brillhart scheme.

CONCLUSIONS

We have found no way of constructing a realistic computing scheme for the discrete logarithm problem, based on the ideas in [1]. As a consequence, contrary to what is stated there, we doubt indeed that it could be possible to compute any logarithm modulo a 200 bit prime by means of the Adleman algorithm within 2.6 days on a 1 μs per operation machine, even if this 'operation' should be an exponentiation modulo the specific prime.

We also think that the algorithm cannot be a serious threat to the public key distribution systems used by Time and Space [12] and Rockwell-Collins [13], utilizing a 256 bit prime.

References

[1] L Adleman: "A subexponential algorithm for the discrete logarithm problem with applications to cryptography" (Working abstract), MIT/LCS, 1979. A shortened and slightly altered version appeared in Proc 20th IEEE Symp on Found of Comp Sci, Oct 1979, p 55-60.

[2] T Herlestam and R Johannesson: "On computing logarithms over $GF(2^p)$", BIT 21(1981), 326-334.

[3] G H Hardy and E M Wright: An Introduction to the Theory of Numbers, 5th ed, Oxford, 1979.

[4] R A Rankin: "The difference between consecutive prime numbers", J London Math Soc 13(1938), 242-247.

[5] N G deBruijn: "On the number of positive integers $\leq x$ and free of prime factors $> y$", Indag Math 13(1951), 50-60.

[6] N G deBruijn: "On the number of positive integers $\leq x$ and free of prime factors $> y$, II", Indag Math 28(1966), 239-247.

[7] V Ennola: "On numbers with small prime divisors", Ann Acad Sci Fennicae (A) I, 440(1969), 1-16.

[8] H Halberstam: "On integers all of whose prime factors are small", Proc London Math Soc (3) 21(1970), 102-107.

[9] A G Konheim: Cryptography, A Primer, Wiley, New York (1981).

[10] M Morrison and J Brillhart: "A method of factoring and the factorization of F_7", Math Comp 29(1975), 183-205.

[11] J D Dixon: "Asymptotically fast factorization of integers", Math Comp 36 (1981), 255-260.

[12] J P Burg and D C Campbell: "Secure voice communication over the public switched network using public key distribution systems", Intelcon 1979 Exp Proc, Dallas 1979, 23-25.

[13] D B Hovden and L G Muret: "User oriented voice security", Intelcon 1979 Exp Proc, Dallas, 1979, 8-9.