BIT 19 (1979), 274–275

CRITICAL REMARKS ON "CRITICAL REMARKS ON SOME PUBLIC-KEY CRYPTOSYSTEMS" BY T. HERLESTAM

RONALD L. RIVEST

Tore Herlestam, in his note "Critical Remarks on Some Public-Key Cryptosystems", [5] suggests a method for attacking the RSA public-key cryptosystem. In this note we show that Herlestam's proposed attack is highly impractical, and that his analysis is erroneous.

The RSA cryptosystem [1] encodes a message M using the key (e,n) via the equation:

$$C \equiv E_n^e(M) \equiv M^e \pmod{n}\,. \tag{1}$$

Here the original message M and the ciphertext C are considered as integers in the range 0 to $n-1$. The integer n is the product of two large prime numbers p and q. The integer e is relatively prime to $(p-1)(q-1)$.

To decrypt a received ciphertext C the recipient computes

$$M \equiv D_n^d(M) \equiv C^d \pmod{n} \tag{2}$$

where d is chosen to satisfy the equation

$$de \equiv 1 \pmod{\operatorname{lcm}(p-1,q-1)}\,.$$

The attack proposed by Herlestam runs as follows: Let $P(x)$ be a polynomial in x such that

$$P(x) = xQ(x)\,. \tag{3}$$

If a given ciphertext C happens to satisfy the equation

$$C^{P(e)} \equiv C \pmod{n} \tag{4}$$

then the corresponding message can be obtained from

$$C^{Q(e)} \equiv M \pmod{n}\,. \tag{5}$$

The actual proposed attack is: given a ciphertext C one wishes to decipher, one tries to find a polynomial $P(x)$ such that (4) holds, and then use (5) to obtain M.

Herlestam bases his optimism for the success of the proposed method in part on his misunderstanding of a lemma in my response to a proposed attack on the RSA system by Simmons and Norris [2, 3]. Let G_n be the multiplicative group of

Received April 4, 1979.

integers mod n. That is, G_n consists of those $\varphi(n)=(p-1)(q-1)$ integers in the range 1 to $n-1$ which are relatively prime to n. The order $\text{order}_n(x)$ of an element $x \in G_n$ is the least $k>0$ such that $x^k \equiv 1 \pmod n$. Elementary group theory tells us that k must divide $\varphi(n)$. If $n=pq$ where $p=a'p'+1$, $q=b'q'+1$, p' and q' are large primes, and a' and b' are small, then the odds are overwhelming that $p'q'$ divides k. Since $G_n=G_p \times G_q$, we have that $\text{order}_n(x)=\text{lcm}(\text{order}_p(x), \text{order}_q(x))$. The number of x in G_p such that p' does not divide $\text{order}_p(x)$ is $\sum_{k|a'} \varphi(k)=a'$ (see [4]). Thus the number of x in G_n whose order is not divisible by $p'q'$ is $a'(q-1)+b'(p-1)-a'b'$, so the probability that $p'q'$ does not divide $\text{order}_n(x)$ is $(p'+q'-1)/p'q'$. This is on the order of 10^{-90}.

Herlestam assumed that the probability that $\text{order}_n(x)=k$, where k divides $a'p'b'q'$, is inversely proportional to the number of divisors of $a'p'b'q'$. This error leads him to incorrectly conclude that the probability that $\text{order}_n(x)$ is not divisible by $p'q'$ is roughly 3/4, instead of 10^{-90}, and to grossly overestimate the chances of success of his attack.

Herlestam further suggests using polynomials $P(x)$ of the form $P(x)=x^a+x^b$ where a and b are distinct small positive integers, so that $Q(x)=x^{a-1}+x^{b-1}$.

For (4) to hold $P(e)$ must be divisible by $\text{order}_n(C)$. In light of our analysis above, we expect this to require (with probability $1-10^{-90}$) $p'q'$ to divide $P(e)$. The chance that this will happen is on the order of $(p'q')^{-1} \cong 10^{-180}$, assuming that $P(e)$ is essentially random in $0,\ldots,\text{lcm}(p-1,q-1)$ as a function of a and b.

Finally, we observe that if Herlestam could find a $P(x)$ such that (4) holds then he would be able to factor n, since $(m!)^2P(e)$ will be divisible by $\varphi(n)$ whenever $p'q'$ divides $P(e)$ and $a',b' \leq m$. By Miller's results such a multiple of $\varphi(n)$ enables one to factor n. Thus his attack can be seen as a (very inefficient) factoring method.

Herlestam's remarks that "numerous simulations carried out by the author ... imply that the corresponding density of fixed points is significant." Since he does not present his evidence, we conclude on the basis of the above argument that he was probably misled by using trivial examples where n has at most a few digits.

REFERENCES

1. R. L. Rivest, A. Shamir and L. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, CACM 21 (Feb. 1978), 120–126.
2. G. J. Simmons and J. J. Norris, *Preliminary Remarks on the M.I.T. Cryptosystem*, Cryptologia 1(4) (1977), 406–414.
3. R. L. Rivest, *Remarks on a Proposed Cryptanalytic Attack on the M.I.T. Public-Key Cryptosystem*, Cryptologia 2(1) (Jan. 1978), 62–65.
4. W. J. LeVeque, *Fundamentals of Number Theory*, Addison–Wesley, 1977.
5. T. Herlestam, *Critical Remarks on some Public-Key Cryptosystems*, BIT 18 (1978), 493–496.

MIT LABORATORY FOR COMPUTER SCIENCE
545 TECHNOLOGY SQUARE
CAMBRIDGE, MASSACHUSETTS 02139
USA