An observation on the Schwenk-Eisfeld public-key encryption scheme

Yvo Desmedt
Dept. EE & CS
University of Wisconsin –
Milwaukee, WI 53201, U.S.A.

Matthew Franklin
AT&T Research
Murray Hill, NJ, USA

We observe that in the Schwenk-Eisfeld scheme [4] (which is a generalization of RSA [3] and Rabin [2]), when $k = 2$ the ciphertext is $c(x) = x^2 - c_1 x + c_2 = x^2 - (m_1 + m_2)x + m_1 \cdot m_2 \bmod n$, since $c(x) = (x - m_1)(x - m_2) \bmod n$, where m_1 and m_2 are plaintext blocks with added redundancy. We focus *only* on $c_1 = m_1 + m_2 \bmod n$.

Observe that in the running key cipher [1] the ciphertext $c = m_1 \oplus m_2$ where m_1 is the plaintext (to be encrypted) and m_2 is the secret key, but the secret key is itself a readable text (plaintext). It is well known that the running key cipher is very vulnerable to a ciphertext-only attack. This attack generalizes to the Schwenk-Eisfeld scheme.

In the Schwenk-Eisfeld scheme $c_1 = m_1 + m_2$ or $c_1 = m_1 + m_2 - n$. The cryptanalyst first guesses which of the two cases to use (if this turns out to be the wrong choice, this can later be corrected). As in the cryptanalysis of the running key cipher, one now uses frequent digrams and tests whether a part of the ciphertext is the sum of two frequent digrams. When these are added in the running key cipher there is no carry, while here there is. The solution to this problem is that one guesses the carry (observe that if one adds the least significant bits of m_1 and of m_2 there is no initial carry). The rest is as for the running key cipher.

References

[1] D. E. R. Denning. *Cryptography and Data Security.* Addison-Wesley, Reading, MA, 1982.

[2] M. Rabin. Digitalized signatures and public-key functions as intractable as factorization. Technical report, Massachusetts Institute of Technology Technical Report MIT/LCS/TR–212, Cambridge, Massachusetts, January 1977.

[3] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public key cryptosystems. *Commun. ACM*, 21, pp. 294–299, April 1978.

[4] J. Schwenk and J. Eisfeld. Public key encryption and signature schemes based on polynomials over Z_n. In U. Maurer, editor, *Advances in Cryptology — Eurocrypt '96, Proceedings (Lecture Notes in Computer Science 1070)*, pp. 60–71. Springer-Verlag, May 12–16, 1996. Zaragoza, Spain.