BREAKING THE CADE CIPHER

N.S. James
Department of Mathematics
University of Tasmania
Hobart, Tasmania 7001
Australia

R. Lidl
Department of Mathematics
University of Tasmania
Hobart, Tasmania 7001
Australia

H. Niederreiter
Kommission für Mathematik
Austrian Academy of Sciences
A-1010 Vienna
Austria

Abstract: A cryptanalysis is given of a cryptosystem introduced by J.J. Cade, which is based on solving equations over finite fields.

In 1985 J.J. Cade [1] introduced a new public-key cryptosystem. The Cade cryptosystem is a public-key cipher in which each block is a string of n binary digits or equivalently an element of the finite field $\mathbb{F}_{2^n}$. Because of the design of the system n must be a multiple of 3, say n = 3c. The blocks are enciphered by a permutation of $\mathbb{F}_{2^n}$ induced by a polynomial $P \in \mathbb{F}_{2^n}[x]$ of the following form,

$$P(x) = p_{00}x^2 + p_{10}x^{q+1} + p_{11}x^{2q} + p_{20}x^{q^2+1} + p_{21}x^{q^2+q} + p_{22}x^{2q^2}$$

where $q = 2^c$ and $p_{00},\ldots,p_{22} \in \mathbb{F}_{q^3}[x]$. The six coefficients $p_{00},\ldots,p_{22}$ are the public-key. The trapdoor information is a decomposition

$$P(x) \equiv S \circ M \circ T(x) \bmod (x^{q^3} - x). \qquad (1)$$

S and T are both linearized polynomials,

$$T(x) = a_0x + a_1x^q + a_2x^{q^2},$$

$$S(x) = b_0x + b_1x^q + b_2x^{q^2},$$

where $a_0,\ldots,b_2 \in \mathbb{F}_{q^3}$ are the private key.

S and T are linear mappings of $\mathbb{F}_{q^3}$, considered as a vector space over $\mathbb{F}_q$ and are both chosen to be invertible. A necessary and sufficient condition for a linearized

Research by the first two authors partially supported by Australian Research Grants Scheme grant No. F8415183.

A.M. Odlyzko (Ed.): Advances in Cryptology - CRYPTO '86, LNCS 263, pp. 60-63, 1987.

polynomial $L(x) = \sum_{s=0}^{r-1} d_i x^{q^i} \in \mathbb{F}_{q^r}[x]$ to be invertible is that $\det A \neq 0$, where

$$A = \begin{pmatrix} d_0 & d_{r-1}^{q} & d_{r-2}^{q^2} & \cdots & d_1^{q^{r-1}} \\ d_1 & d_0^{q} & d_{r-1}^{q^2} & \cdots & d_2^{q^{r-1}} \\ \cdot & \cdot & \cdot^{q^2} & \cdot & \cdot^{q^{r-1}} \\ d_{r-1} & d_{r-2}^{q} & d_{r-3}^{q^2} & \cdots & d_0^{q^{r-1}} \end{pmatrix} .$$

In the Cade cipher we have $q = 2^c$ and $r = 3$. The set of linearized polynomials over $\mathbb{F}_{q^r}$ forms a group under composition mod $(x^{q^r}-x)$, called the Betti-Mathieu group, which is isomorphic to the general linear group of nonsingular r by r matrices with entries in $\mathbb{F}_q$, see [3] for details on linearized polnomials. We note that P(x) in (1) is obtained mod $(x^{q^3}-x)$. Therefore polynomial decomposition algorithms for finding the secret composition factors S, M and T are not applicable. M is the special monomial $M(x) = x^{q+1}$ which is invertible because $(q+1, q^3-1) = 1$ for $q = 2^c$. T, M and S are easy to invert and so $P^{-1} = T^{-1} \circ M^{-1} \circ S^{-1}$ is easy to calculate if one knows the private key.

We now give a method for finding the private key $a_0,\ldots,b_2$ in terms of the public key $p_{00},\ldots,p_{22}$.

From (1) we have

$$\begin{aligned} P \circ T^{-1}(x) &\equiv S \circ M(x) \bmod (x^{q^3}-x) \\ &\equiv b_0 x^{q+1} + b_2 x^{q^2+1} + b_1 x^{q^2+q} . \end{aligned} \tag{2}$$

Because T is a linearized polynomial T^{-1} will have the same form as T. In fact

$$T^{-1}(x) = \alpha_0 x + \alpha_1 x^{q} + \alpha_2 x^{q^2}$$

where

$$\begin{aligned} \alpha_0 &= (a_0^{q^2+q} + a_1^{q} a_2^{q^2})/A , \\ \alpha_1 &= (a_2^{q^2+1} + a_0^{q^2} a_1)/A , \\ \alpha_2 &= (a_1^{q+1} + a_0^{q} a_2)/A , \end{aligned} \tag{3}$$

and $$A = a_0^{q^2+q+1} + a_1^{q^2+q+1} + a_2^{q^2+q+1} + a_0a_1^qa_2^{q^2} + a_0^qa_1^{q^2}a_2 + a_0^{q^2}a_1a_2^q .$$

We may then calculate $P \circ T^{-1}(x)$. This has six terms and comparison of the coefficients of these terms with those in (2) yields the following equations:

$$\left.\begin{aligned} b_0 &= p_{10}(\alpha_0^{q+1} + \alpha_1\alpha_2^q) + p_{20}(\alpha_1^{q^2+1} + \alpha_0\alpha_2^{q^2}) \\ &\quad + p_{21}(\alpha_2^{q^2+q} + \alpha_0^q\alpha_1^{q^2}) , \\ b_2 &= p_{10}(\alpha_2^{q+1} + \alpha_0\alpha_1^q) + p_{20}(\alpha_0^{q^2+1} + \alpha_1^{q^2}\alpha_2) \\ &\quad + p_{21}(\alpha_1^{q^2+q} + \alpha_0^{q^2}\alpha_2^q) , \\ b_1 &= p_{10}(\alpha_1^{q+1} + \alpha_0^q\alpha_2) + p_{20}(\alpha_2^{q^2+1} + \alpha_0^{q^2}\alpha_1) \\ &\quad + p_{21}(\alpha_0^{q^2+q} + \alpha_1^q\alpha_2^{q^2}) , \end{aligned}\right\} \tag{4}$$

$$\left.\begin{aligned} &p_{00}\alpha_0^2 + p_{11}\alpha_2^{2q} + p_{22}\alpha_1^{2q^2} + p_{10}\alpha_0\alpha_2^q \\ &\quad + p_{20}\alpha_0\alpha_1^{q^2} + p_{21}\alpha_1^{q^2}\alpha_2^q = 0 , \\ &p_{11}\alpha_0^{2q} + p_{22}\alpha_2^{2q^2} + p_{00}\alpha_1^2 + p_{21}\alpha_0^q\alpha_2^{q^2} \\ &\quad + p_{10}\alpha_0^q\alpha_1 + p_{20}\alpha_1\alpha_2^{q^2} = 0 , \\ &p_{22}\alpha_0^{2q^2} + p_{00}\alpha_2^2 + p_{11}\alpha_1^{2q} + p_{20}\alpha_0^{q^2}\alpha_2 \\ &\quad + p_{21}\alpha_0^{q^2}\alpha_1^q + p_{10}\alpha_1^q\alpha_2 = 0 . \end{aligned}\right\} \tag{5}$$

Now if we raise the second and third equations of (5) to the powers q^2 and q respectively and put $\alpha = \alpha_0$, $\beta = \alpha_2^q$, $\gamma = \alpha_1^{q^2}$ then we obtain

$$\left.\begin{aligned} &p_{00}\alpha^2 + p_{11}\beta^2 + p_{22}\gamma^2 + p_{10}\alpha\beta + p_{20}\alpha\gamma + p_{21}\beta\gamma = 0 , \\ &p_{11}^{q^2}\alpha^2 + p_{22}^{q^2}\beta^2 + p_{00}^{q^2}\gamma^2 + p_{21}^{q^2}\alpha\beta + p_{10}^{q^2}\alpha\gamma + p_{20}^{q^2}\beta\gamma = 0 , \\ &p_{22}^q\alpha^2 + p_{00}^q\beta^2 + p_{11}^q\gamma^2 + p_{20}^q\alpha\beta + p_{21}^q\alpha\gamma + p_{10}^q\beta\gamma = 0 . \end{aligned}\right\} \tag{6}$$

If one of α, β or γ is zero then the equations are easy to solve. This can be detected a priori, e.g. if $\gamma = 0$ then necessarily

$$\det\begin{pmatrix} p_{00} & p_{11} & p_{10} \\ p_{11}^q & p_{22}^q & p_{21}^q \\ p_{22}^q & p_{00}^q & p_{20}^q \end{pmatrix} = 0.$$

Thus assume $\alpha\beta\gamma \neq 0$. Because the equations in (6) are homogeneous we may assume $\gamma = 1$. Using two of the equations in (6) to eliminate the α^2 term we obtain

$$\alpha(c_1\beta + c_2) + c_3\beta^2 + c_4\beta + c_5 = 0 \qquad (7)$$

for some $c_1,\ldots,c_5 \in \mathbb{F}_q$.

If $c_1 = c_2 = 0$ then we have a quadratic equation for β. Such an equation can be solved by treating this case as an affine polynomial and use of the method described in [4, p.103], or alternatively use the method of Exercise 4.44 in [4, p.161].

Otherwise we may substitute for α in one of the equations in (6) and so obtain a quartic equation for β. A quartic equation over $\mathbb{F}_{2^n}$ may be solved by the method described in Chen [2]. Equations (3) and (4) then give the values of a_0,a_1,a_2 and b_0,b_1,b_2 respectively.

We understand from the originator of the Cade cipher that S. Berkovits has developed an alternative method of breaking the cipher. An improved version of the cipher has been presented at CRYPTO 86.

REFERENCES

1. Cade, J.J.; A public key cipher which allows signatures. Paper presented at 2nd SIAM Conference on Applied Linear Algebra, Raleigh 1985.

2. Chen, Chin-Long; Formulas for the solutions of quadratic equations over GF(2^m), IEEE Trans. Inform. Theory 28, 792-794 (1982).

3. Lidl, R. and Niederreiter, H.; Finite Fields. Addison-Wesley, Reading, Mass. 1983. Now distributed by Cambridge University Press.

4. Lidl, R. and Niederreiter, H.; Introduction to Finite Fields and Their Applications. Cambridge University Press, Cambridge, 1986.