ON CRYPTOSYSTEMS BASED ON POLYNOMIALS AND FINITE FIELDS

R. Lidl (University of Tasmania, Australia)

ABSTRACT

In many single-key, symmetric or conventional cryptosystems the elements of a finite field can be regarded as the characters of a plaintext and ciphertext alphabet. Some properties of polynomials or polynomial functions on finite fields can be used for constructing cryptosystems. This note demonstrates by way of examples that great care has to be taken in choosing polynomials for enciphering and deciphering. Often complex looking polynomial functions induce very simple permutations of the elements of a finite field and therefore are not suitable for the construction of cryptosystems. Also an indication is given of some further areas of research in algebraic cryptography.

1. BINOMIALS

There are several examples of cryptosystems that involve polynomials and finite fields; see e.g. [1], [4], [6], [8]. We have to confine our choice of polynomials to a relatively small class of polynomials because of two reasons: the polynomial $f(x)$ should induce a permutation of the elements of a finite field F_q; that is $f: F_q \to F_q$, $a \to f(a)$ should be a permutation. Polynomials $f(x)$ with this property are called *permutation polynomials*. Second, the inverse of f should be easy to compute for deciphering purposes by the authorized receiver. These two requirements of f considerably narrow the choice of polynomials.

Monomials x^k have been studied repeatedly as to their suitability for cryptography. In public-key (asymmetric) cryptosystems the RSA scheme uses the corresponding polynomial functions as enciphering and deciphering functions modulo an integer n. Some conventional exponentiation ciphers use the difficulty of calculating discrete logarithms for finite fields.

We consider *binomials* for conventional cryptosystems and show that their usefulness is very limited. Let

$$(1) \qquad f(x) = ax^k + bx$$

where $k > 2$ is fixed independently of a prime power q. Niederreiter and Robinson [13] showed that no binomial of this form is a permutation polynomial of F_q for sufficiently large q. In detail:

T. Beth, N. Cot, and I. Ingemarsson (Eds.): Advances in Cryptology - EUROCRYPT '84, LNCS 209, pp. 10-15, 1985.

<u>*THEOREM*</u> *([13], p.209). Let $k > 2$. Then:*

(i) if k is not a prime power, then for all finite fields F_q with $q \geq (k^2-4k+6)^2$ there is no permutation polynomial of F_q of the form (1) over F_q with $ab \neq 0$,

(ii) if k is a power of the prime p, then for all finite fields F_q with $q \geq (k^2-4k+6)^2$ and characteristic not equal to p there is no permutation polynomial of F_q of the form (1) over F_q with $ab \neq 0$.

This result can be generalized to polynomials of the form $ax^k + bx^j \in F_q[x]$, $ab \neq 0$, $1 \leq j < k$, see [13, p.211]. Again, for sufficiently large q none of these binomials is a permutation polynomial of F_q.

Since the above results hold for k being independent of q, let us consider the situation where k is of the form $(q+1)/2$, q odd. Then the family of polynomial functions in $F_q[x]$ of the form

$$f(x) = ax^{(q+1)/2} + bx \tag{2}$$

is closed under composition. It is easily verified that for two polynomials $f_i(x) = a_i x^{(q+1)/2} + b_i x$, $i = 1,2$, we have

$$(f_1 \circ f_2)(x) = f_1(f_2(x)) \equiv (a_1 c + b_1 a_2) x^{(q+1)/2} + (a_1 d + b_1 b_2) x \pmod{(x^q - x)},$$

where $c + d = (a_2+b_2)^{(q+1)/2}$ and $c - d = (b_2-a_2)^{(q+1)/2}$. Thus it is possible to easily find the inverse $g(x)$ of a given polynomial $f(x)$ of the form (2) from $f(x) \circ g(x) = x$, $g(x) \circ f(x) = x$. In [13] it is shown that a polynomial $f(x) = x^{(q+1)/2} + bx \in F_q[x]$ is a permutation polynomial of F_q if and only if $b^2 - 1$ is a nonzero square in F_q. So it appears that polynomials of the form (2) may be suitable candidates for enciphering functions in a cryptosystem. We note, however, that the mappings of F_q into itself which are induced by permutation polynomials (2) are very simple, since $f(s) = (a+b)s$ for a square $s \in F_q$ and $f(t) = (b-a)t$ for a non-square $t \in F_q$. Therefore the mapping f is linear on the squares or non-squares of F_q.

It may be fruitful to study binomials on the integers mod n and use them in RSA type cryptosystems instead of monomials x^k.

2. CHEBYSHEV POLYNOMIALS OF THE SECOND KIND

Several generalizations of the RSA cryptosystem have been suggested based on different enciphering functions; see [1], [9] and [12]. In some of these papers Chebyshev polynomials of the first kind (or Dickson polynomials, as they are called in an algebraic/number theoretic context) and their multivariate generalization play a central role. Here we consider Chebyshev polynomials of the second kind as to their suitability for constructing cryptosystems over F_q. The *Chebyshev polynomial* $f_k(x)$ *of the second kind* is defined by

$$f_k(x) = \sum_{i=0}^{\lfloor k/2 \rfloor} \binom{k-i}{i} (-1)^i \, x^{k-2i} \quad .$$

We note that $f_k(x)$ is a polynomial of degree k with integer coefficients. Alternative ways of defining the polynomials $f_k(x)$ are by recursive equations

$$f_{k+2}(x) - xf_{k+1}(x) + f_k(x) = 0 \quad \text{with } f_0(x) = 1,\ f_1(x) = x \ ;$$

or by the functional equation

$$f_k(x) = (u^{k+1} - u^{-(k+1)})/(u-u^{-1})$$

where $x = u + u^{-1}$ and $u \neq \pm 1$,

$$f_k(2) = k + 1 \text{ and } f_k(-2) = (-1)^k(k+1).$$

The following result gives sufficient conditions to ensure that $f_k(x)$ induces a permutation of F_q. Let $q = p^e$, p an odd prime.

<u>*THEOREM*</u> *(Matthews [11]). The polynomial $f_k(x)$ is a permutation polynomial of F_q if k satisfies the congruences*

(3) $k + 1 \equiv \pm 2 \pmod p$, $k + 1 \equiv \pm 2 \pmod{\tfrac12(q-1)}$, $k + 1 \equiv \pm 2 \pmod{\tfrac12(q+1)}$.

<u>Proofidea.</u> Let S be the subset of F_{q^2} consisting of all solutions of equations of the form $x^2 - ax + 1 = 0$, $a \in F_q$. Then $= \{u \in F_{q^2} | u^{q-1} = 1 \text{ or } u^{q+1} = 1\}$. The integer k must be odd, since either $\tfrac12(q-1)$ or $\tfrac12(q+1)$ is even. Thus $f_k(-x) = f_k(x)$. Let $u \in F_{q^2}$ and $u^2 - xu + 1 = 0$. If $u^{q-1} = 1$, then $u^{\frac12(q-1)} = \pm 1$. Now, if $u^{\frac12(q-1)} = 1$, then $u^{k+1} = u^2$ or $u^{k+1} = u^{-2}$, since $k + 1 \equiv \pm 2 \pmod{\tfrac12(q-1)}$. Therefore $f_k(x) = (u^2-u^{-2})/(u-u^{-1}) = u + u^{-1} = x$, or $f_k(x) = -(u+u^{-1}) = -x$. The remaining cases $u^{\frac12(q-1)} = -1$, $u^{q+1} = 1$ and $u = \pm 1$ are treated similarly. □

It follows that f_k is its own inverse:

$$(f_k \circ f_k)(x) = f_k(f_k(x)) = x, \text{ whenever } k \text{ satisfies (3).}$$

Here the composite $f_k(f_k(x))$ is reduced modulo $x^q - x$. This would be a suitable property for a symmetric cryptosystem with secret key k. The above proof, however, shows that the mapping of F_q into itself induced by a permutation polynomial $f_k(x)$ is not very complex at all, since $f_k(-a) = -f_k(a)$ and $f_k(a) = a$ or $-a$ for each $a \in F_q$. So the complicated enciphering function f_k induces a simple permutation of F_q.

3. COMMUTING POLYNOMIAL VECTORS

In order to implement digital signatures it is useful if the enciphering function E and the deciphering function D commute with respect to substitution; that is $E \circ D = D \circ E$. If E_i and D_i are the enciphering function and deciphering function, respectively, of person i then these functions are easy to handle if we require

$$E_i \circ E_j = E_j \circ E_i,\ E_i \circ D_j = D_j \circ E_i,\ D_i \circ D_j = D_j \circ D_i.$$

This leads to studying *commuting* or *permutable polynomials*. In [9] all possible classes of commuting polynomials in one variable were determined according to their suitability in RSA-type cryptosystems. Because of the following result, the classical Chebyshev polynomials $T_n(x)$ of the first kind are of special interest. Bertram showed (see e.g. Rivlin [15, p.161]) that over an integral domain R of characteristic zero, if $n \geq 2$ and the polynomial f(x) of degree $k \geq 1$ commutes under substitution with $T_n(x)$, then $f(x) = T_k(x)$ if n is even and $f(x) = \pm T_k(x)$ if n is odd. (A similar result holds if char R = p). A two-dimensional generalization of this theorem was derived in [9]. We say that two polynomial vectors (f_1,f_2) and (g_1,g_2) in $R[x,y]^2$ commute if

$$(f_1(g_1,g_2),\ f_2(g_1,g_2)) = (g_1(f_1,f_2),\ g_2(f_1,f_2)).$$

In short

$$(f_1,f_2) \circ (g_1,g_2) = (g_1,g_2) \circ (f_1,f_2).$$

In [8], [9] or [10] a two-dimensional generalization of the Chebyshev polynomials $T_n(x)$ is presented in terms of a polynomial vector $(g_k(x,y),\ \bar{g}_k(x,y))$ or $(g_k,\bar{g}_k)$ for short. Let R be an integral domain of a characteristic that does not divide $n \geq 2$. Then the following generalizes Bertram's result:

<u>*THEOREM*</u> *([7]).* *If $f \in (\mathbb{R}[x,y])^2$ is of degree $k \geq 1$, then f commutes with $(g_n,\bar{g}_n)$ if and only if f is of the form*

$$f = (\alpha g_k, \alpha^2 \bar{g}_k) \quad \text{or} \quad f = (\alpha \bar{g}_k, \alpha^2 g_k)$$

where $\alpha = 1$ if $n \not\equiv 1 \pmod 3$ or $\alpha^3 = 1$ if $n \equiv 1 \pmod 3$.

In the one-variable case all classes of commuting polynomials (so-called permutable chains) have been determined (see e.g. Lausch and Nöbauer [5] and [9]). The corresponding classification in the case of polynomial vectors in two variables is still an open problem. The Theorem above is a first result in this direction. Commuting polynomial vectors can be used for digital signatures analogous to the one-dimensional situation described in [9].

<u>4. FURTHER PROBLEM AREAS</u>

Brawley, Carlitz and Levine [2] have determined the polynomials $f(x) \in F_q[x]$ which permute the set $F_q^{n\times n}$ of $n\times n$ matrices with entries in F_q under substitution, that is $f : F_q^{n\times n} \to F_q^{n\times n}$, $A \longrightarrow f(A)$ is a permutation of matrices.

<u>*THEOREM*</u> *([2]).* *The polynomial $f(x) \in F_q[x]$ is a permutation polynomial of $F_q^{n\times n}$ if and only if*

(i) $f(x)$ is a permutation of F_{q^r}, $1 \leq r \leq n$; and

(ii) $f'(x)$ does not vanish on any of the fields $F_q,\ldots,F_{q^{\lfloor n/2 \rfloor}}$.

Such permutation polynomials could be used for enciphering plaintext messages which are arranged in matrix form. A first step would be to determine specific polynomials $f(x)$ which are suitable as enciphering functions of such cryptosystems.

A different problem area is concerned with the study of iterative roots of functions over finite fields. The *iterates* of a function $g : F_q \to F_q$ are defined inductively by $g^0(x) = x$ and $g^n(x) = g(g^{n-1}(x))$, $n > 0$. If f is another function on F_q, with the property $g^n = f$, $n \geq 2$, then g is called an *iterative root of order n* of f or an nth iterative root of f. In [3] the existence of iterative roots of f are investigated for special types of functions, such as linear functions, power function x^k and Chebyshev polynomials of the first kind. Apart from theoretical existence theorems (developed in [3]) it could be potentially useful in cryptography to explicitly determine iterative roots of given functions. Our interest in this topic arose from the question: "When is $f(f(z)) = az^2 + bz + c$ for all complex numbers z ?" Rice, Schweizer and Sklar [14] showed that the answer is: never.

References

1. Brändström H.: A public-key cryptosystem based upon equations over a finite field. Cryptologia 7 (1983) 347-358.

2. Brawley, J.V., L. Carlitz and J. Levine: Scalar polynomial functions on the n×n matrices over a finite field. Linear Alg. Appl.10 (1975) 199-217.

3. Dunn, K.B. and R. Lidl: Iterative roots of functions over finite fields. Math. Nachrichten (to appear).

4. Ecker, A.: Über die mathematischen Grundlagen einiger Chiffrierverfahren. Computing 29 (1982) 277-287.

5. Lausch, H. and W. Nöbauer: Algebra of Polynomials. North Holland, Amsterdam 1973.

6. Levine, J. and J.V. Brawley: Some cryptographic applications of permutation polynomials. Cryptologia 1 (1977) 76-92.

7. Lidl, R. and G.L. Mullen: Commuting polynomial vectors over an integral domain (to appear).

8. Lidl, R. and W.B. Müller: A note on polynomials and functions in algebraic cryptography. Proceedings 11th Australian Conference of Combinatorial Mathematics. Ars Combinatoria (to appear).

9. Lidl, R. and W.B. Müller: Permutation polynomials in RSA-cryptosystems. Proceedings CRYPTO '83 Santa Barbara. Plenum Publ. (to appear).

10. Lidl, R. and H. Niederreiter: Finite Fields. Encyclopedia of Mathematics and its Applications vol.20. Addison-Wesley, Reading, Massachusetts 1983.

11. Matthews, R.: Permutation polynomials in one and several variables. Ph.D. thesis, University of Tasmania, 1983.

12. Müller, W.B. and W. Nöbauer: Some remarks on public-key cryptosystems. Studia Sci. Math. Hungar. 16 (1981) 71-76.

13. Niederreiter, H. and K.H. Robinson: Complete mappings of finite fields. J. Austral. Math. Soc. (Series A) 33 (1982) 197-212.

14. Rice, R.E., B. Schweizer and A. Sklar: When is $f(f(z)) = az^2+bz+c$ for all complex z? Amer. Math. Monthly 87 (1980) 252-263.

15. Rivlin, T.J.: The Chebyshev Polynomials. J. Wiley & Sons, New York, 1974.

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