Int. J. Appl. Math. and Comp. Sci., 1999, Vol.9, No.4, 955–963

A QUASIGROUP-BASED PUBLIC-KEY CRYPTOSYSTEM

CZESŁAW KOŚCIELNY*, GARY L. MULLEN**

A public-key cryptosystem, using generalized quasigroup-based streamciphers is presented. It is shown that such a cryptosystem allows one to transmit securely both a cryptogram and a secret portion of the enciphering key using the same insecure channel. The system is illustrated by means of a simple, but non-trivial, example.

Keywords: quasigroups, latin squares, cryptography, streamciphers

1. Introduction

We discuss a public-key cryptosystem based upon properties of quasigroups. Assuming a quasigroup Q as a secret portion of an encryption key, our quasigroup-based streamcipher allows the user to simultaneously transmit over the same insecure channel, the cryptogram as well as a public portion of the enciphering key. This property can be taken into account while constructing protocols for public-key cryptosystems which employ quasigroup-based streamciphers. Such public-key cryptosystems, however, have somewhat different properties than e.g. the RSA system. In our system, a group of users, having the same secret portion of the enciphering key can both encode and decode messages, and so members of this group should trust each other. Another group of users sharing the same communication channel may have another portion of the key. Neither of the two groups can decode messages from the other group and so this type of system should be useful. Among the many possible protocols, we provide a non-trivial example in Section 3.

We remind the reader that quasigroups are equivalent to the more familiar Latin squares in that the multiplication table of a quasigroup of order q is a latin square of order q, and conversely as indicated in Dénes and Keedwell (1974), every latin square of order q is the multiplication table of a quasigroup of order q.

* Technical University of Zielona Góra, Department of Robotics and Software Engineering, ul. Podgórna 50, 65–246 Zielona Góra, Poland, e-mail: C.Koscielny@irio.pz.zgora.pl

** Mathematics Department, The Pennsylvania State University, University Park, PA 16802, USA, e-mail: mullen@math.psu.edu

2. Quasigroup-Based Generalized Streamciphers

The streamciphers discussed in this paper are generalized in the sense that they can be constructed over any alphabet A of q symbols, q denoting an arbitrary integer ≥ 3. Let

$$Q = \langle A, \oplus \rangle \tag{1}$$

be an arbitrary quasigroup with $|A| = q$, and let

$$M = m_1 \; m_2 \; \cdots \; m_i \; \cdots \tag{2}$$

$$K = k_1 \; k_2 \; \cdots \; k_i \; \cdots \tag{3}$$

$$C = c_1 \; c_2 \; \cdots \; c_i \; \cdots \tag{4}$$

denote the stream of characters of the plaintext, the stream of characters of the secret key and the stream of characters of the cryptogram, respectively. The characters of these three streams belong, of course, to the set A.

To generate the stream of characters of the cryptogram, a generalized streamcipher uses an enciphering function f_e so that

$$c_i = f_e(m_i, k_i), \tag{5}$$

which, for each character m_i of the plaintext and for the character k_i of the key associated with it, determines a character c_i of the cryptogram. During deciphering a function f_d is used: it reconstructs the character m_i of the message, taking into account the character c_i of the cryptogram and the corresponding character k_i of the key so that

$$m_i = f_d(c_i, k_i). \tag{6}$$

It is obvious that

$$f_d\Big(f_e(m_i, k_i), k_i\Big) = m_i \tag{7}$$

must be satisfied for all $i = 1, 2, \ldots, n$, where n denotes the number of characters in the plaintext.

Now it will be shown how the operation in a quasigroup can be applied to deliver invertible transformations needed for the streamciphers. The addition table of a quasigroup Q can be used as the table of values of a discrete bi-variate function $\mathcal{S}$, for which

$$\mathcal{S}(x, y) = x \oplus y, \qquad \mathcal{S}(y, x) = y \oplus x, \tag{8}$$

where $\oplus$ denotes the operation in the quasigroup Q. Here the first variable corresponds to the row entry, while the second variable corresponds to the column entry. Using (8) one can define two operators ($\ominus$ and $\oslash$) for performing 'subtraction' in a quasigroup Q:

$$\mathcal{S}(x, y) \ominus y = x, \qquad \mathcal{S}(y, x) \oslash y = x. \tag{9}$$

We introduce two more functions $\mathcal{D}$ and $\widehat{\mathcal{D}}$ defined by

$$\mathcal{D}(x,y) = x \ominus y, \tag{10}$$

$$\widehat{\mathcal{D}}(x,y) = x \oslash y. \tag{11}$$

It follows immediately from (8)–(11) that

$$D\Big(\mathcal{S}(x,y),y\Big) = x, \tag{12}$$

$$\widehat{\mathcal{D}}\Big(\mathcal{S}(y,x),y\Big) = x. \tag{13}$$

One can also prove that

$$S\Big(\mathcal{D}(x,y),y\Big) = x, \tag{14}$$

$$\widehat{\mathcal{D}}\Big(y,\mathcal{D}(y,x)\Big) = x, \tag{15}$$

$$D\Big(y,\widehat{\mathcal{D}}(y,x)\Big) = x, \tag{16}$$

$$\mathcal{S}\Big(y,\widehat{\mathcal{D}}(x,y)\Big) = x. \tag{17}$$

Taking into consideration (8)–(17) and property (7), one can observe that the six pairs of functions

$$(\mathcal{S},\mathcal{D}), \quad (\mathcal{S},\widehat{\mathcal{D}}), \quad (\mathcal{D},\widehat{\mathcal{D}}), \quad (\mathcal{D},\mathcal{S}), \quad (\widehat{\mathcal{D}},\mathcal{S}), \quad (\widehat{\mathcal{D}},\mathcal{D}) \tag{18}$$

form six pairs of invertible transformations, which can be used as an enciphering and deciphering pair (f_e, f_d). Thus if a quasigroup Q is not Abelian, then for the same plaintext M and the same key K there may exist up to six distinct cryptograms. This is a substantial improvement to the usual streamcipher built over $GF(2)$, where the unique operation XOR is usually applied.

3. An Example

We now consider a larger example. Suppose that one wants to construct a quasigroup-based generalized streamcipher using the following 32-character alphabet:

$$A = \texttt{ABCDEFGHIJKLMNOPQRSTUVWXYZ:,.!?-}$$

and the quasigroup of order 32 with the operation table in the form of a function, $\mathcal{S}(x,y)$, given in Table 1 which is the multiplication table for the quasigroup $Q = \langle A, \oplus \rangle$. The function $\mathcal{S}(x,y) = x \oplus y$ and eqns. (12) and (13) determine the functions $\mathcal{D}(x,y)$ and $\widehat{\mathcal{D}}(x,y)$, shown in Tables 2 and 3, respectively.

Assuming that the plaintext has the form

$$M = \texttt{THIS-PLAINTEXT-IS-A-SHORT-MESSAGE-TO-BE-ENCRYPTED}$$

Table 1. Function $\mathcal{S}(x,y)$.

$\mathcal{S}(x,y)$	y A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	:	,	.	!	?	-
A	K	I	.	U	Z	T	-	O	G	M	D	Y	E	?	:	C	X	W	!	Q	P	F	R	V	J	,	H	A	L	S	N	B
B	L	!	U	Y	O	G	H	R	T	,	M	:	B	C	?	-	Z	P	A	N	V	S	J	X	I	Q	E	D	K	F	.	W
C	N	S	B	Z	H	V	C	:	X	L	Q	W	I	F	U	Y	E	A	,	-	M	K	G	T	?	D	P	O	R	!	J	.
D	!	Q	?	G	U	M	Y	N	,	T	E	V	-	H	I	F	D	S	C	Z	:	.	W	L	B	O	J	R	P	A	X	K
E	D	?	E	,	C	W	.	-	P	S	I	R	N	B	H	Z	G	T	U	O	!	J	:	A	M	X	Q	L	Y	V	K	F
F	X	F	Y	?	K	P	N	D	V	:	S	,	Q	U	A	.	R	!	I	H	T	L	-	M	O	Z	W	B	G	E	C	J
G	W	Y	L	X	,	J	:	A	I	B	P	F	K	!	.	V	-	M	E	C	O	N	S	?	T	R	U	Q	Z	D	H	G
H	Z	M	D	P	G	?	,	L	C	H	X	I	.	T	V	Q	K	B	O	:	U	Y	A	F	!	N	-	S	J	W	R	E
I	T	U	H	A	R	K	O	I	L	!	F	B	J	Z	S	G	C	D	Q	V	X	?	Y	N	W	-	.	,	:	M	E	P
J	A	D	S	T	F	U	E	W	Y	G	R	H	C	P	Q	:	J	,	L	B	?	-	K	Z	X	!	M	.	O	N	V	I
K	S	G	X	Q	W	:	L	B	?	I	C	-	R	V	T	!	M	H	N	J	A	E	,	U	.	P	F	K	D	Z	O	Y
L	B	O	!	H	E	Y	U	M	:	V	K	T	Z	I	-	N	.	R	S	D	,	Q	L	W	F	G	A	C	X	J	P	?
M	?	V	R	-	:	F	A	H	S	.	W	Q	U	Y	E	,	I	J	Z	P	L	T	C	K	N	M	O	X	B	G	D	!
N	H	:	T	S	-	.	V	Z	U	?	N	!	W	D	X	O	A	E	P	I	Y	R	F	B	L	K	,	J	M	C	G	Q
O	.	C	,	M	V	H	R	?	E	J	!	A	G	-	F	I	N	Q	D	K	W	O	X	P	U	B	T	Y	S	:	L	Z
P	Y	Z	F	K	I	R	P	Q	J	W	O	L	D	A	,	?	U	:	.	E	-	C	T	G	S	V	X	M	!	H	B	N
Q	:	E	M	O	N	L	F	U	K	P	H	X	?	J	D	A	Q	Y	-	,	G	B	!	R	Z	C	S	W	T	.	I	V
R	V	W	I	B	L	Q	!	G	N	Z	.	D	X	:	J	M	F	O	R	T	H	P	E	-	C	U	K	?	,	Y	S	A
S	J	A	W	C	Y	E	M	S	B	-	:	Z	T	.	R	P	V	N	F	X	Q	U	D	I	K	H	G	!	?	O	,	L
T	F	L	N	R	A	D	G	Y	M	E	T	K	:	X	C	B	?	I	V	.	S	W	O	Q	P	J	!	U	H	-	Z	,
U	M	X	C	N	Q	S	K	,	F	A	-	J	O	W	Z	R	P	V	B	Y	E	G	H	!	D	L	:	I	.	T	?	U
V	C	,	A	J	B	X	W	!	Z	D	?	.	V	K	M	L	T	G	:	F	R	I	U	E	-	S	N	H	Q	P	Y	O
W	I	P	Z	W	.	O	J	T	R	N	Y	M	S	L	B	K	!	-	X	G	D	H	Q	:	A	E	?	V	U	,	F	C
X	U	T	:	D	J	I	B	P	!	Q	L	O	A	M	G	H	,	?	K	W	F	V	Z	S	Y	.	C	N	E	X	-	R
Y	P	R	Q	I	D	B	X	C	W	K	,	?	L	E	Y	S	O	F	H	A	J	!	N	.	G	:	Z	-	V	U	M	T
Z	-	.	K	!	?	,	I	E	Q	O	J	G	H	N	P	W	S	X	Y	U	Z	M	V	D	R	T	B	F	C	L	A	:
:	Q	K	P	L	M	!	?	X	A	C	V	S	F	O	N	J	:	U	T	R	I	Z	.	,	E	Y	D	G	-	B	W	H
,	E	-	G	V	!	N	Q	F	.	X	Z	P	,	R	O	U	Y	K	W	S	C	D	B	J	H	A	L	:	I	?	T	M
.	O	B	V	E	S	-	T	J	H	Y	G	U	M	,	L	D	W	.	?	!	N	A	P	C	:	I	R	Z	F	K	Q	X
!	G	H	O	:	X	C	D	K	-	F	B	N	P	Q	!	T	L	Z	J	M	.	,	?	Y	V	W	I	E	A	R	U	S
?	,	N	J	.	P	A	Z	V	D	R	U	C	!	S	K	E	H	L	G	?	B	X	M	O	Q	F	Y	T	W	I	:	-
-	R	J	-	F	T	Z	S	.	O	U	A	E	Y	G	W	X	B	C	M	L	K	:	I	H	,	?	V	P	N	Q	!	D

Table 2. Function $\mathcal{D}(x, y)$.

	y																												
$\mathcal{D}(x,y)$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	:	,	.	!	?	-
A	J	S	V	I	T	?	M	G	:	U	-	O	X	P	F	Q	N	C	B	Y	K	.	H	E	W	,	L	A	!	D	Z	R
B	L	.	C	R	V	Y	X	K	S	G	!	I	B	E	W	T	-	H	U	J	?	Q	,	N	D	O	Z	F	M	:	P	A
C	V	O	U	S	E	!	C	Y	H	:	K	?	J	B	T	A	I	-	D	G	,	P	M	.	R	Q	X	L	Z	N	F	W
D	E	J	H	X	Y	T	!	F	?	V	A	R	P	N	Q	.	D	I	O	L	W	,	S	Z	U	C	:	B	K	G	M	-
E	,	Q	E	.	L	S	J	Z	O	T	D	-	A	Y	M	?	C	N	G	P	U	K	R	V	:	W	B	!	X	F	I	H
F	T	F	P	-	J	M	Q	,	U	!	I	G	:	C	O	D	R	Y	S	V	X	A	N	H	L	?	K	Z	.	B	W	E
G	!	K	,	D	H	B	T	R	A	J	.	Z	O	-	X	I	E	V	?	W	Q	U	C	P	Y	L	S	:	F	M	N	G
H	N	!	I	L	C	O	B	M	.	H	Q	J	Z	D	E	X	?	K	Y	F	R	W	U	-	,	S	A	V	T	P	G	:
I	W	A	R	Y	P	X	Z	I	G	K	E	H	C	L	D	O	M	T	F	N	:	V	-	S	B	.	!	U	,	?	Q	J
J	S	-	?	V	X	G	W	.	P	O	Z	U	I	Q	R	:	J	M	!	K	Y	E	B	,	A	T	D	N	H	L	C	F
K	A	:	Z	P	F	I	U	!	Q	Y	L	T	G	V	?	W	H	,	X	O	-	C	J	M	S	N	R	K	B	.	E	D
L	B	T	G	:	R	Q	K	H	I	C	X	P	Y	W	.	V	!	?	J	-	M	F	L	D	N	U	,	E	A	Z	O	S
M	U	H	Q	O	:	D	S	L	T	A	B	W	.	X	V	R	K	G	-	!	C	Z	?	F	E	M	J	P	N	I	Y	,
N	C	?	T	U	Q	,	F	D	R	W	N	!	E	Z	:	L	O	S	K	B	.	G	Y	I	M	H	V	X	-	J	A	P
O	.	L	!	Q	B	W	I	A	-	Z	P	X	U	:	,	N	Y	R	H	E	G	O	T	?	F	D	M	C	J	S	K	V
x P	Y	W	:	H	?	F	P	X	E	Q	G	,	!	J	Z	S	U	B	N	M	A	R	.	O	T	K	C	-	D	V	L	I
Q	:	D	Y	K	U	R	,	P	Z	X	C	M	F	!	J	H	Q	O	I	A	S	L	W	T	?	B	E	G	V	-	.	N
R	-	Y	M	T	I	P	O	B	W	?	J	E	K	,	S	U	F	L	R	:	V	N	A	Q	Z	G	.	D	C	!	H	X
S	K	C	J	N	.	U	-	S	M	E	F	:	W	?	I	Y	Z	D	L	,	T	B	G	X	P	V	Q	H	O	A	R	!
T	I	X	N	J	-	A	.	W	B	D	T	L	S	H	K	!	V	E	:	R	F	M	P	C	G	Z	O	?	Q	U	,	Y
U	X	I	B	A	D	J	L	Q	N	-	?	.	M	F	C	,	P	:	E	Z	H	S	V	K	O	R	G	T	W	Y	!	U
V	R	M	.	,	O	C	N	?	F	L	:	D	V	K	H	G	S	U	T	I	B	X	Z	A	!	P	-	W	Y	E	J	Q
W	G	R	S	W	K	E	V	J	Y	P	M	C	N	U	-	Z	.	A	,	X	O	T	D	L	I	!	F	Q	?	H	:	B
X	F	U	K	G	!	V	Y	:	C	,	H	Q	R	T	N	-	A	Z	W	S	I	?	O	B	J	E	P	M	L	X	D	.
Y	P	G	F	B	S	L	D	T	J	.	W	A	-	M	Y	C	,	Q	Z	U	N	H	I	!	X	:	?	O	E	R	V	K
Z	H	P	W	C	A	-	?	N	V	R	,	S	L	I	U	E	B	!	M	D	Z	:	X	J	Q	F	Y	.	G	K	T	O
:	Q	N	X	!	M	K	G	C	L	F	S	B	T	R	A	J	:	P	V	H	D	-	E	W	.	Y	U	,	I	O	?	Z
,	?	V	O	E	G	Z	H	U	D	B	Y	F	,	.	P	M	X	J	C	Q	L	!	K	:	-	A	N	I	R	W	S	T
.	O	Z	A	?	W	N	E	-	,	M	R	V	H	S	G	F	L	.	P	T	!	D	:	Y	K	X	I	J	U	Q	B	C
!	D	B	L	Z	,	:	R	V	X	I	O	N	?	G	!	K	W	F	A	.	E	Y	Q	U	H	J	T	S	P	C	-	M
?	M	E	D	F	Z	H	:	O	K	N	V	Y	Q	A	B	P	T	X	.	?	J	I	!	G	C	-	W	R	S	,	U	L
-	Z	,	-	M	N	.	A	E	!	S	U	K	D	O	L	B	G	W	Q	C	P	J	F	R	V	I	H	Y	:	T	X	?

Table 3. Function $\widehat{\mathcal{D}}(x,y)$.

	y																											
$\widehat{\mathcal{D}}(x,y)$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	:	,	.	!	?	-
A	,	S	R	!	X	O	H	W	D	A	U	:	G	Q	L	N	P	-	B	E	J	C	Y	M	T	?	I	Z	V	.	F	K
B	-	M	C	Y	N	,	J	R	L	T	H	A	.	X	Z	?	V	D	I	P	S	E	O	G	F	:	!	W	B	K	U	Q
C	P	N	G	S	E	?	T	I	Q	M	K	,	W	!	B	V	Z	Y	D	O	C	A	-	:	H	.	J	U	X	F	L	R
D	K	,	Z	Q	A	H	!	C	R	B	.	T	?	N	S	M	O	L	W	F	Y	J	U	D	E	X	:	V	P	G	I	-
E	M	:	Q	K	C	!	S	-	?	G	V	E	O	R	I	T	B	W	F	J	U	X	Z	.	N	H	Y	A	D	,	P	L
F	V	!	N	P	-	B	L	X	K	E	:	Y	F	W	O	C	G	Q	S	A	I	T	?	U	R	,	M	H	.	J	Z	D
G	I	F	W	D	Q	.	-	E	P	J	B	Z	!	?	M	X	U	H	:	G	V	R	T	O	Y	L	,	C	K	A	S	N
H	:	G	E	N	O	T	?	J	C	L	R	D	H	A	F	!	K	U	Z	.	W	,	V	P	S	M	-	Y	I	B	Q	X
I	B	Y	M	O	K	S	I	L	H	-	J	N	Q	T	P	E	?	C	X	R	,	V	A	F	D	G	U	.	Z	:	!	W
J	Y	W	?	:	V	-	F	.	M	Q	T	!	R	,	J	I	N	O	A	Z	L	D	G	E	U	K	P	X	H	S	C	B
K	A	.	V	-	?	E	M	Q	F	W	,	K	X	Z	T	D	I	:	Y	L	G	N	P	S	J	C	B	R	!	H	O	U
L	.	A	J	X	,	V	C	H	I	S	G	W	U	Y	?	L	F	E	-	B	Z	P	N	K	M	!	D	:	O	Q	R	T
M	J	K	U	F	Y	X	R	B	!	:	Q	H	Z	.	D	,	C	P	G	I	A	O	L	N	?	V	E	-	M	T	W	S
N	?	T	A	H	M	G	V	Z	X	!	S	P	Y	K	Q	-	E	I	R	C	D	:	J	,	W	N	O	F	U	L	B	.
O	H	E	,	Z	T	Y	U	S	G	.	?	B	:	P	V	K	D	R	!	W	M	-	F	L	Q	J	N	O	A	C	X	I
P	U	R	:	.	I	F	K	D	-	N	Z	?	T	S	X	G	J	V	P	Y	Q	!	B	H	A	O	C	L	W	M	E	,
Q	T	Z	K	B	:	M	,	P	S	O	D	V	L	-	R	H	Q	F	U	X	E	.	W	J	C	I	A	G	?	N	Y	!
R	W	H	.	,	L	Q	Z	?	E	K	M	R	C	V	G	F	X	S	O	D	P	U	I	-	B	Y	T	N	:	!	J	A
S	!	V	B	R	J	K	W	,	O	C	A	S	I	D	.	Y	:	?	H	U	F	Z	M	X	P	Q	L	T	E	-	N	G
T	F	I	X	J	R	U	Y	N	A	D	O	L	V	C	:	W	.	T	M	K	!	Q	H	B	-	Z	S	?	G	P	,	E
U	D	C	O	E	S	N	:	U	B	F	X	G	M	I	Y	Q	H	Z	V	,	-	W	.	A	!	T	R	P	L	?	K	J
V	X	U	F	L	!	I	P	O	T	?	N	J	B	G	E	Z	-	A	Q	S	R	M	,	V	.	W	K	D	C	Y	H	:
W	R	-	L	W	F	:	A	!	Y	H	E	X	K	M	U	J	,	B	C	V	N	G	D	T	I	P	?	S	Q	Z	.	O
X	Q	X	I	?	Z	A	D	K	U	Y	C	.	,	O	W	:	L	M	T	N	B	F	S	!	G	R	H	J	-	E	V	P
Y	L	D	P	G	.	C	B	V	W	I	-	F	N	U	,	A	R	!	E	H	T	?	K	Y	O	S	Z	Q	J	X	:	M
Z	E	Q	D	T	P	Z	.	A	N	X	!	M	S	H	-	B	Y	J	L	?	O	I	C	W	:	U	V	K	,	R	G	F
:	O	L	H	U	W	J	G	T	.	P	F	I	E	B	!	R	A	N	K	M	:	S	X	C	Z	-	Q	,	Y	D	?	V
,	Z	J	S	I	D	L	E	G	,	R	W	U	P	:	C	O	T	.	?	-	H	B	!	Q	K	F	X	M	N	V	A	Y
.	C	?	-	V	G	P	O	M	:	,	Y	Q	J	F	A	S	!	K	N	T	.	L	E	Z	X	B	W	I	R	U	D	H
!	S	B	!	A	U	R	N	Y	J	Z	P	C	-	L	K	.	W	G	,	:	X	H	Q	I	V	D	F	E	T	O	M	?
?	N	O	Y	C	B	D	X	F	V	U	I	-	A	J	H	P	M	,	.	Q	?	K	:	R	L	E	G	!	S	W	T	Z
-	G	P	T	M	H	W	Q	:	Z	V	L	O	D	E	N	U	S	X	J	!	K	Y	R	?	,	A	.	B	F	I	-	C

then, using a key

$$K = \texttt{KJ?JRFFUAPGLMICCBGGEZ-NVDITCOMBSJCWOCSH,,QMI-TNRA}$$

and the function $\mathcal{S}(M,K)$ as an encrypting transformation, the following cryptogram:

$$C_1 = \mathcal{S}(M,K) = \texttt{THE-CRYPTOGRAM-HAS-THE-PROPERTIES-OF-A-PLAINTEXT!}$$

is obtained. The reader will verify without difficulty that $\mathcal{D}(C_1,K)$ returns M. This case may be considered as a masquerade cipher, because C_1 is easily readable and comprehensible.

Using the same message M and the same key K, five other cryptograms can be obtained as follows:

$$C_2 = \mathcal{S}(K,M) = \texttt{JWDLA.,MGACEKV.XAGWFY.XGZP:HDZLMF.GF.AGM!JRD,BILU}$$

$$C_3 = \mathcal{D}(M,K) = \texttt{THQEWFQKWL.-RB-RCAMNV::NJ!!EIWS?T-P,-UZY!OJWKMHNE}$$

$$C_4 = \mathcal{D}(K,M) = \texttt{O.K!XDGX:JWRFNWHUG!HME:ULJSEH-L-XWX,WCCTG!QTV!BII}$$

$$C_5 = \widehat{\mathcal{D}}(M,K) = \texttt{OL!CXFVJB-YE,ATMVQHHQXPUJZIQ.IS:GTHVTI-BAEWEMYCWK}$$

$$C_6 = \widehat{\mathcal{D}}(K,M) = \texttt{L.VAACYDDSG,NRRQINILL:QAFWVE!G-WVRVVRVOYD-UC,WCL!}$$

While deciphering these cryptograms one must remember that

$$M = \widehat{\mathcal{D}}(C_2,K) = \mathcal{S}(C_3,K) = \widehat{\mathcal{D}}(K,C_4), = \mathcal{S}(K,C_5) = \mathcal{D}(K,C_6), \quad (19)$$

which follows directly from (12)–(17).

If now one knows only the quasigroup Q, but does not know the proper key K and tries to decrypt the cryptogram C_2 using the key

$$K_r = \texttt{YXTT!G?!-QRQ:TTZ-PRD,PPGAIVERBHYQHIQGK!JAVAMHMNIO}$$

then he will obtain

$$M_1 = \mathcal{S}(C_2,K_r) = \texttt{X:ZDSTTGGXAGFF!.BV-?-DH:-JZGS.MNRJIRTDD.G-V-FBZ:Z}$$

$$M_2 = \mathcal{D}(C_2,K_r) = \texttt{ALL-DESIGN-CRITERIA-OF-THE-CIPHER-ARE-MADE-PUBLIC}$$

$$M_3 = \widehat{\mathcal{D}}(C_2,K_r) = \texttt{UTFB.OATNPYBBSTRKXBPQS:-E-SOLQH?GMPGOUA:SDW?G.TIY}$$

$$M_4 = \widehat{\mathcal{D}}(K_r,C_2) = \texttt{ISJLSK!-QT.:FQGWGKIHKWH-?EK-,:DNMIIMKANR.?-FYKXNM}$$

$$M_5 = \mathcal{D}(K_r,C_2) = \texttt{OJLDFR?A:MUSMQJZPAT-DOT,O-ZTOJ-RTZRFARIDLCOVHRHG}$$

$$M_6 = \mathcal{S}(K_r,C_2) = \texttt{KZRKGZTPS:INVWHDRPEMH!G:,GN-BQILLJOLZSDCSDW-SVUBW}$$

Decrypting correctly C_1 with the key

$K_s = \texttt{KJCCVSWTRI?PGKHUKU:RFWHTAFUFAXPRCH,AK-H.TSD.YMBM,}$

yields

$$Ms = \mathcal{D}(C_1,K_s) = \texttt{THE-PRIME-NUMBER-THEOREM-WAS-CONJECTURED-BY-GAUSS}$$

4. Implementation

We briefly describe the results of an implementation of our system based upon the use of a quasigroup of order 256. The block scheme of the encrypting procedure, based on 8-bit byte serial transmission is shown in Fig. 1. The encrypting procedure is accomplished as follows:

Step 1. Block X generates at random k_x bytes which are transformed by a secret function F into the seed for the known at the receiving end random byte generator RNG. The switch is in position 1 and k_x bytes are transmitted to the output C. In the meantime RNG generates k_d random bytes, stored in the memory D.

Step 2. The switch is in position 2. Random byte generator RNG continues to generate the stream of random bytes, which is passed to the first input of two-input quasigroup operator $\mathcal{S}$ (see Tab. 1), while the delayed output of RNG is supplied to the second input of this operator. Thus at the output of the block $\mathcal{S}$ a stream of bytes of key K appears, and the second two-input quasigroup operator $\mathcal{S}$ produces the stream of bytes of cryptogram C using the stream of bytes of the plaintext M. This step is repeated till all the bytes of plaintext are exhausted.

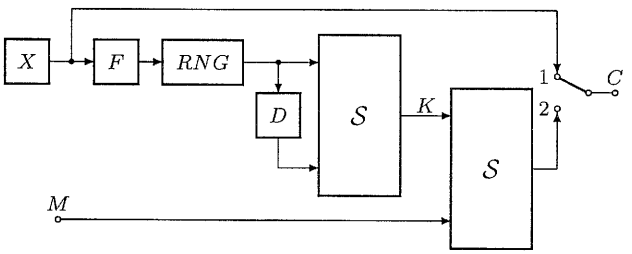

Fig. 1. Block scheme of the encryption procedure.

The decrypting procedure works in a similar manner. According to Fig. 2, this procedure consists of the following two steps:

Step 1. The switch is in position 1. After receiving k_x random bytes, the initial conditions for RNG are reconstructed.

Step 2. The switch is in position 2; the quasigroup operator $\mathcal{D}$ (see Tab. 2), using K and C, delivers to the output the stream of the bytes of plaintext M.

Each step of this procedure can be implemented by hardware or by means of appropriate software. Implementing the presented algorithms in Pascal, the encrypting and decrypting speeds listed in Tab. 4 have been obtained.

It follows that the method presented here, implemented by means of a specialized microprocessor system, can satisfy almost all persons searching for very fast and secure cryptograhic devices.

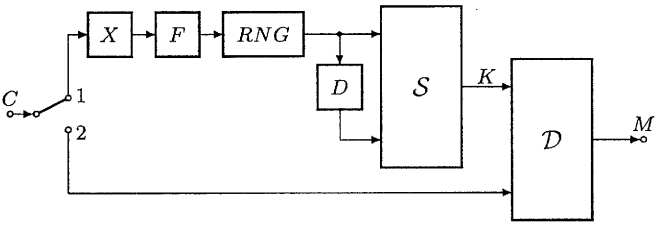

Fig. 2. Block scheme of the decryption procedure.

Table 4. The speed of executing enciphering and deciphering procedures on various PC computers.

IBM PC type	**encryption**	**decryption**
Pentium II 333 Mhz 64 MB RAM	8188.00 kbps	7792.96 kbps
Pentium 100 MHz 24 MB RAM	1926.08 kbps	2351.84 kbps
486DX4 100 MHz 16 MB RAM	1094.72 kbps	866.08 kbps
386 DX 8 MB RAM	377.44 kbps	367.84 kbps

References

Beth T., Frish M. and Simmons G.J. (1992): *Public Key Cryptography: State of the Art and Future Directions.* — Lecture Notes in Computer Science, Vol.578, Berlin: Springer-Verlag.

Dénes J. and Keedwell A.D. (1974): *Latin Squares and Their Applications.* — Budapest: Akadémiai Kiadó; New York: Academic Press.

Hsu D.F. (1980): *Cyclic Neofields and Combinatorial Designs.* — Lecture Notes in Mathematics, Vol.824, Berlin: Springer-Verlag.

Laywine C.F. and Mullen G.L. (1998): *Discrete Mathematics Using Latin Squares.* — New York: Wiley.

Kościelny C. (1996): *A Method of Constructing Quasigroup-Based Stream-Ciphers.* — Appl. Math. Comp. Sci., Vol.6, No.1, pp.109–121.

Simmons G.J. (Ed.) (1992): *Contemporary Cryptology.* — The Science of Information Integrity, New York: IEEE Press.

Received: 23 April 1999
Revised: 17 August 1999