Crossed-inverse quasigroups with long inverse cycles and applications to cryptography

A. D. Keedwell
Department of Mathematics and Statistics
University of Surrey, Guildford GU2 5XH, Surrey, U.K.

Abstract In this paper, we show that crossed-inverse quasigroups have certain properties which make them particularly appropriate for use in cryptography. In particular, we provide a construction for crossed-inverse quasigroups with long inverse cycles and describe some applications.

I. INTRODUCTION.

A finite quasigroup $(Q,\ o)$ of order n consists of a set Q of symbols on which a binary operation (o) is defined such that (i) for all pairs of elements $a,b \in Q$, $aob \in Q$ (*closure*) and (ii) for all pairs $a,b \in Q$, there exist unique elements $x,y \in Q$, such that $xoa = b$ and $aoy = b$ (*unique solubility of equations*).

A quasigroup may satisfy some or all of the following:
(i) for all $a,b,c \in Q$, $(aob)oc = ao(boc)$ (*the associative law*);
(ii) for all $a,b \in Q$, $aob = boa$ (*the commutative law*);
(iii) there exists an element $e \in Q$ such that, for all $a \in Q$, $eoa = a = aoe$ (*existence of a two-sided identity element*);
(iv) for each $a \in Q$, there exists an element $a_L^{-1} \in Q$ such that $a_L^{-1}o(aob) = b$ for all $b \in Q$ (*the left inverse property*);
(v) for each $a \in Q$, there exists an element $a_R^{-1} \in Q$ such that $(boa)oa_R^{-1} = b$ for all $b \in Q$ (*the right inverse property*);
(vi) for each $a \in Q$, there exists an element $a'_L \in Q$ such that $a'_L o(boa) = b$ for all $b \in Q$ (*the left crossed-inverse property*);
(vii) for each $a \in Q$, there exists an element $a'_R \in Q$ such that $(aob)oa'_R = b$ for all $b \in Q$ (*the right crossed-inverse property*).

Some of the above properties are inter-dependent. The most important of the connections for our purposes are the following:
(a) A quasigroup which satisfies (i) is called a *group*. If it also satisfies (ii), it is an *abelian group*. Every group satisfies (iii), (iv), (v). If and only if it is abelian, the group also satisfies (vi), (vii).
(b) A quasigroup which satisfies (iii) is called a *loop*. An associative loop is a group.
(c) A quasigroup which satisfies (iv) and (v) is called an *inverse-property quasigroup*. One which satisfies (vi) and (vii) is called a *crossed-inverse-property quasigroup*. For a quasigroup which is commutative, (iv)⇔(vi) and (v)⇔(vii) so the inverse and crossed inverse properties coincide.

Lemma 1.1: A quasigroup $(Q,\ o)$ of finite order which has the left crossed-inverse property also has the right crossed-inverse property; and conversely.

Proof: The left crossed-inverse property states that, for every element $a \in Q$, there exists an element $a'_L \in Q$ such that $a'_L\, o(boa) = b$ for every $b \in Q$. To each $a \in Q$, there corresponds a unique a'_L because the equation $xo(boa) = b$ has a unique solution $x = a'_L$. Also, distinct elements $a_1, a_2 \in Q$ have distinct left inverses because $(a_1')_L = (a_2')_L = a'_L$ would imply $a'_L\, o(boa_1) = b = a'_L\, o(boa_2)$ and so, by the unique solubility of equations, $boa_1 = boa_2$ whence $a_1 = a_2$. It follows that, given $c \in Q$, there exists a unique $c' \in Q$ such that $co(boc') = b$ for all $b \in Q$. Let d be an arbitrary element of Q. By the solubility of equations, there exists an element $b \in Q$ such that $d = boc'$. Then, $cod = co(boc') = b$ and so $(cod)oc' = boc' = d$. That is, given $c \in Q$, there exists an element $c' \in Q$ such that $(cod)oc' = d$ for all $d \in Q$. This is the right crossed-inverse property.

The proof of the converse is similar.

In this paper, we shall be especially interested in non-commutative quasigroups of finite order which satisfy (vi) and consequently (by Lemma 1.1) also satisfy (vii). For brevity, we shall call them *CI-quasigroups* as, for example, in [1] and [2].

From now onwards, we shall write a' to denote the right crossed-inverse of the element a in a CI-quasigroup. Note that, from Lemma 1.1, $(cob)oc' = b \Leftrightarrow co(boc') = b$ so, if c' is the right crossed-inverse of c, then c is the left crossed-inverse of c'.

Lemma 1.2: If a_L^{-1} is the left inverse of a in a quasigroup (Q, o) which has the left inverse property, then a is the left inverse of a_L^{-1} for that quasigroup. An analogous result holds for right inverses.

Proof: By the left inverse property, $a_L^{-1} o(aoc) = c$ for all $c \in Q$. Let b be an arbitrary element of Q. Then, by the solubility of equations, there exists an element $c \in Q$ such that $b = aoc$. So $a_L^{-1} ob = a_L^{-1} o(aoc) = c$, whence $ao(a_L^{-1} ob) = aoc = b$. This proves the result because b was arbitrarily chosen.

In the applications to be described later in this paper, it is assumed that the message to be transmitted can be represented as a single element m of a quasigroup (Q, o) and that this is enciphered by multiplying it by another element a of (Q, o) so that the encoded message is am. At the receiving end, the message is deciphered by multiplying by the inverse of a. If a right (or left) inverse property quasigroup is used and the right (left) inverse of a is a' say, then the right (left) inverse of a' is necessarily a. If a CI-quasigroup is used, this is not necessarily the case (as we shall show). This fact makes an attack on the system more difficult in the latter case.

Definition. If (Q, o) is a CI-quasigroup in which a' is the right crossed-inverse of a, a'' is that of a', a''' is that of a'', and so on, then the cycle $(a\, a'\, a'' \ldots)$ is called the *inverse cycle* associated with the element a.

R. Artzy [1] was the first to study the possible lengths of the inverse cycles of a CI-quasigroup though, in fact, he considered only loops. He proved, among other things, that if the inverse cycles of a CI-loop of order n consist of (e), where e is the identity element of the loop, and one other cycle (of length $n-1$) then $n = 2$ or 3. (In other words, only the cyclic groups C_2 and C_3 have this property. Compare corollary II of our Theorem 2.1 below.) He also showed that, if a CI-loop has an inverse cycle of length $r > 2$, it has another inverse cycle distinct from (e) whose length is a (not-necessarily proper) factor of r. (That is, the factor of r may be r itself or 1.) As illustrations of this result, he gave a CI-loop of order 9 whose non-identity inverse cycles have lengths 2 and 6 and two non-isomorphic CI-loops of order 10 whose non-identity inverse cycles have lengths 1 and 8. The latter examples demonstrate the existence of of CI-loops with inverse cycles of maximum possible length $n-2$ (when $n > 3$). We reproduce one of these examples in Figure 1.1 below. The inverse cycles are (e), (1) and (2 3 4 5 6 7 8 9).

In [2], Artzy proved that isotopic CI-loops are isomorphic. Later, in [3], V. D. Belousov and B.V. Tzurkan showed that, if every loop isotopic to a given CI-loop is again a CI-loop, then the loop must in fact be an abelian group.

(o)	*e*	1	2	3	4	5	6	7	8	9
e	*e*	1	2	3	4	5	6	7	8	9
1	1	*e*	8	9	2	3	4	5	6	7
2	2	4	7	*e*	6	9	5	8	3	1
3	3	5	1	8	*e*	7	2	6	9	4
4	4	6	5	1	9	*e*	8	3	7	2
5	5	7	3	6	1	2	*e*	9	4	8
6	6	8	9	4	7	1	3	*e*	2	5
7	7	9	6	2	5	8	1	4	*e*	3
8	8	2	4	7	3	6	9	1	5	*e*
9	9	3	*e*	5	8	4	7	2	1	6

Fig. 1.1.

The above facts concerning isomorphism suggest that CI-quasigroups which are not loops may be of most value in our cryptographic application. In the next section, we shall show how such quasigroups may be constructed.

II. Main Theorem.

Theorem 2.1: Let $(G, .)$ be an abelian group of order n such that $n+1$ is composite. Define a binary operation (o) on the elements of G by the relation $aob = a^r b^s$, where $rs = n+1$. Then (G, o) is a CI-quasigroup and the right crossed inverse of the element a is a^u, where $u = (-r)^3$.

Corollary I: If $(G, .)$ is the cyclic group C_p of prime order p and there exists a divisor r of $p+1$ such that $(-r)^3$ is a primitive root of p, then the inverse cycles of (G, o) are of lengths 1 and $p-1$. (An earlier conjecture of the author was that such a divisor r exists whenever $p \equiv 2 \bmod 3$. However, for $p > 1000$, counterexamples exist. One obtained by R. K. Guy[8] to whom the author posed the problem is $p = 1181$. He does not guarantee that it is the smallest.)

Corollary II: If $(G, .)$ is an elementary abelian group of order p^t (that is, an abelian group in which every element has the same prime order p) and there exists a divisor r of p^t+1 such that $(-r)^3$ is a primitive root of p, then the inverse cycles of (G, o), excepting that of the identity element e of $(G, .)$, all have equal length $p-1$.

Proof: We first show that (G, o) is a quasigroup. Let $xoa = b$. Then $x^r a^s = b$ so $x^r = ba^{-s}$ and $x = x^{rs} = (ba^{-s})^s$ which is an element of G. Similarly, if $aoy = b$, then $a^r y^s = b$ so $y = y^{rs} = (a^{-r}b)^r$. Thus, equations are uniquely soluble and (G, o) is a quasigroup. Also, $(aob)oc = (aob)^r c^s = (a^r b^s)^r c^s = b^{sr} a^{rr} c^s = b$ if $a^{rr} c^s = e$, the identity element of $(G, .)$: that is, if $c^s = a^{-rr}$ or if $c = c^{sr} = a^u$, where $u = (-r)^3$, as before. Thus, (G, o) is a CI-quasigroup and a^u, where $u = (-r)^3$, is the right crossed inverse of a. The result of the theorem follows.

Suppose next that $u = (-r)^3$ is a primitive root of p. Then $(a\ a^u\ a^{uu}\ \ldots)$, of length $p-1$, is the inverse cycle of (G, o) which contains the element a since $u^{p-1} \equiv 1 \bmod p$ and $u^h \neq 1 \bmod p$ for $1 \leq h \leq p-2$. This proves both of the corollaries.

The above theorem provides a means of constructing CI-quasigroups with long inverse cycles and also proves the existence of CI-quasigroups all of whose non-identity cycles have equal length, thus answering for quasigroups the similar question discussed by Artzy for loops.

It is worth observing also that the CI-quasigroups so constructed are isotopes of the abelian group $(G, .)$. We may see this as follows: Since r and s are divisors of $n+1$, they are necessarily prime to the order n of $(G, .)$ and so the mappings $\alpha: x \to x^r$ and $\beta: y \to y^s$ are permutations of G. It follows immediately that (G, o) is an isotope of $(G, .)$ because $xoy = x\alpha . y\beta$.

To illustrate the theorem, we give three examples:

Example 2.1. Let $(G, .)$ be the cyclic group $C_5 = <c: c^5 = e>$ and define $aob = a^3 b^2$. We find that the multiplication table of the CI-quasigroup is as shown in Figure 2.1, where the integers 0, 1, 2, 3, 4 represent the various powers of the generating element c of C_5. Since $u = (-3)^3 \equiv 3 \bmod 5$, $c^u = c^3$, $(c^3)^u = c^4$, $(c^4)^u = c^2$ and $(c^2)^u = c$, so the corresponding decomposition of G into inverse cycles is (0)(1 3 4 2).

Thus, $(0o3)o0 = 1o0 = 3$
$(2o4)o1 = 4o1 = 4$
$(4o2)o2 = 1o2 = 2$
$(3o3)o4 = 0o4 = 3$
etc.

(o)	0	1	2	3	4
0	0	2	4	1	3
1	3	0	2	4	1
2	1	3	0	2	4
3	4	1	3	0	2
4	2	4	1	3	0

Fig. 2.1

Example 2.2. Let $(G, .)$ be the cyclic group $C_{11} = <c: c^{11} = e>$ and define $aob = a^4 b^3$. Then, $(-4)^3 \equiv 2 \bmod 11$ so it is a primitive root and the non-identity element inverse cycle has length 10.

Example 2.3. Let $(G, .)$ be the elementary abelian group $C_5 \times C_5$ and define $aob = a^2 b^{13}$. Then, $(-2)^3 \equiv 2 \bmod 5$ which is a primitive root of 5. The six non-identity element inverse cycles each have length 4.

Note: The CI-quasigroup obtained by the method of Theorem 2.1 is unipotent only if $r+s = n$: that is, only if $n = 5$.

When using an algebraic system for cryptographic purposes, economy of storage is important. We shall show that, in the case of a CI-loop with an inverse cycle of maximum length or of a CI-quasigroup with an inverse cycle of length one less than its order, very compact storage is possible because the structure of the entire quasigroup is determined by that of a single row of the Cayley table of the quasigroup. This is a consequence of the fact that the mapping J of an element to its right crossed-inverse is an automorphism of the quasigroup. Although the latter fact is well-known for the case of loops, the aforementioned implication does not seem to have been noticed until now. In our next theorem, we give a version of the result which is valid for CI-quasigroups as well as for CI-loops. (See also [3].)

Theorem 2.2: For any CI-quasigroup $(Q, \circ)$, the mapping J: $a \rightarrow a'$ from an element to its right crossed-inverse is an automorphism.

Proof: For all pairs a,b of the elements of the quasigroup (or loop), we have $(a \circ b) \circ aJ = b$. Thus, $(c \circ d) \circ cJ = d$. Putting $c = a \circ b$ and $d = aJ$, we get $[(a \circ b) \circ aJ] \circ (a \circ b)J = aJ$. That is, $b \circ (a \circ b)J = aJ$. Then, putting $c = b$ and $d = (a \circ b)J$, we get $[b \circ (a \circ b)J\,] \circ bJ = (a \circ b)J$. That is, $aJ \circ bJ = (a \circ b)J$. This proves the theorem.

We apply this result first to the case of a CI-loop with e as identity element. As we remarked earlier, Artzy has proved that (when $n > 3$) the maximum length of an inverse cycle is $n-2$ and that, when such a maximum length cycle exists, the loop has two self-inverse elements; namely e and another element which we shall denote by σ. Further, we shall suppose that the elements of the loop are denoted by e, 0, 1, ... , $n-3$, σ and that the border elements of its Cayley table are written in that order. Also, we suppose that the notation is chosen so that $(0\ 1\ \ 2\ \dots\ n-3)$ is the long inverse cycle. Thus, $eJ = e$, $\sigma J = \sigma$, and $aJ = (a+1) \bmod (n-2)$ for $a = 0, 1, \dots, n-3$.

Let us suppose that $0 \circ b = \sigma$. Then $0J^r \circ bJ^r = \sigma J^r$ for $r = 1, 2, \dots, n-3$ since J is an automorphism. That is, $r \circ (b+r) = \sigma$ for $r = 0, 1, \dots, n-3$, where addition is modulo $n-2$. Thus, the entries σ lie along a broken left-to-right diagonal of the $(n-2)\times(n-2)$ subsquare of the Cayley table which is formed by the second to $(n-1)$th rows and columns of the table. (See Figure 2.2 for an illustrative example with $n = 10$.) Also, using the crossed inverse property, we find that $0 \circ b = \sigma \Rightarrow b = (0 \circ b) \circ 1 = \sigma \circ 1 \Rightarrow b \circ \sigma = (\sigma \circ 1) \circ \sigma = 1$ so $\sigma J^r \circ 1J^r = bJ^r$ and $bJ^r \circ \sigma J^r = 1J^r$ for $r = 1, 2, \dots, n-3$. Hence, $\sigma \circ r = b+r-1$ and $r \circ \sigma = 1+r-b$ for $r = 0, 1, \dots, n-3$. Thus, the entries of the last row and column of the Cayley table of the loop are all determined by the cell of the second row which contains the entry σ (since this entry defines b).

Next, suppose that $0 \circ 0 = a$. Then, by the crossed inverse property, $0 = (0 \circ 0) \circ 1 = a \circ 1$ and $0 \circ (a+1) = (a \circ 1) \circ (a+1) = 1$, where addition is modulo $n-2$, as before. Since J is an automorphism, $a \circ 1 = 0 \Rightarrow 0 \circ (1-a) = -a$. Thus, $0 \circ 0 = a \Rightarrow 0 \circ (a+1) = 1$ and $0 \circ (-a+1) = -a$.

Similar reasoning shows that $0 \circ c = d \Rightarrow c = (0 \circ c) \circ 1 = d \circ 1$ and $c \circ (d+1) = (d \circ 1) \circ (d+1) = 1$. Thence, using the fact that J is an automorphism, $0 \circ c = d \Rightarrow 0 \circ (1-d) = c-d$ and $0 \circ (d-c+1) = 1-c$. So, since $0 \circ 1 = e$, it is sufficient to specify $\lceil (n-1)/3 \rceil$ of the entries of the second row of the Cayley table in order to determine the remainder. Moreover, because J is an automorphism, $0 \circ c = d \Rightarrow 0J^r \circ cJ^r = dJ^r \Rightarrow r \circ (c+r) = d+r$ for $r = 0, 1, \dots, n-3$ and so these $\lceil (n-1)/3 \rceil$ entries determine the entire Cayley table.

(o)	e	0	1	2	3	4	5	6	7	σ
e	e	0	1	2	3	4	5	6	7	σ
0	0	**5**	e	**4**	7	3	6	1	σ	2
1	1	σ	6	e	5	0	4	7	2	3
2	2	3	σ	7	e	6	1	5	0	4
3	3	1	4	σ	0	e	7	2	6	5
4	4	7	2	5	σ	1	e	0	3	6
5	5	4	0	3	6	σ	2	e	1	7
6	6	2	5	1	4	7	σ	3	e	0
7	7	e	3	6	2	5	0	σ	4	1
σ	σ	6	7	0	1	2	3	4	5	e

Fig. 2.2.

For example, the CI-loop whose Cayley table is given in Figure 2.2 above is completely determined by the statements that $n = 10$ and that $0 \circ 7 = \sigma$, $0 \circ 0 = 5$ and $0 \circ 2 = 4$. The latter loop is isomorphic to that given in Figure 1.1 and can be obtained from it by the mapping $\phi = \begin{pmatrix} e & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ e & \sigma & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix}$.

Similarly, a CI-loop isomorphic to the second example of order 10 given by Artzy in [1] is completely determined by the statements that $n = 10$ and that $0 \circ 7 = \sigma$, $0 \circ 0 = 5$ and $0 \circ 2 = 6$.

Next we consider the case of a CI-quasigroup of order n with elements σ, 0, 1, ... , $n-2$. We choose the notation so that σ is self-inverse and so that $(0\ 1\ 2 \ldots n-2)$ is the long inverse cycle.

Note. We have shown the existence of such CI-quasigroups in Theorem 2.1. CI-quasigroups of order n with a single inverse cycle of length n also exist. More details of these are given elsewhere. (See [4].)

We write the border elements of the Cayley table of our quasigroup in the order 0, 1, ... , $n-2$, σ. Let us suppose that σ occurs in the $(b+1)$th column of the first row of the table so that $0 \circ b = \sigma$. Then $0J^r \circ bJ^r = \sigma J^r$ for $r = 1, 2, \ldots, n-2$ since J is an automorphism. That is, $r \circ (b+r) = \sigma$ for $r = 0, 1, \ldots, n-2$, where addition is modulo $n-1$. Thus, the entries σ lie along a broken left-to-right diagonal of the $(n-1)\times(n-1)$ subsquare of the Cayley table which is formed by its first $n-1$ rows and columns. (An illustrative example is given in Figure 2.3 with $n = 11$.) Also, using the crossed inverse property, we see that $0 \circ b = \sigma \Rightarrow b = (0 \circ b) \circ 1 = \sigma \circ 1 \Rightarrow b \circ \sigma = (\sigma \circ 1) \circ \sigma = 1$ so $\sigma J^r \circ 1J^r = bJ^r$ and $bJ^r \circ \sigma J^r = 1J^r$ for $r = 1, 2, \ldots, n-2$. Hence, $\sigma \circ r = b+r-1$ and $r \circ \sigma = 1+r-b$ for $r = 0, 1, \ldots, n-2$. Thus, the entries of the last row and column of the Cayley table of the quasigroup are all determined by the cell of the first row which contains the entry σ. (Compare the corresponding analysis for loops given above.)

Next, suppose that $0 \circ 0 = a$. By exactly the same reasoning as we used for the case of a CI-loop with a long inverse cycle, $0 \circ 0 = a \Rightarrow 0 \circ (a+1) = 1$ and $0 \circ (-a+1) = -a$. Also, if $0 \circ c = d$, then $0 \circ (1-d) = c-d$ and $0 \circ (d-c+1) = 1-c$. Moreover, each entry of the first row thus obtained determines the complete left-to-right broken diagonal on which it lies. We conclude that the entire CI-quasigroup is determined by the cell of the first row in which σ

lies and by the contents of $\lceil (n-2)/3 \rceil$ other cells of the first row: that is, by a total of $\lceil (n+1)/3 \rceil$ cells.

(o)	0	1	2	3	4	5	6	7	8	9	σ
0	**7**	**5**	**4**	9	3	0	6	8	1	σ	2
1	σ	8	6	5	0	4	1	7	9	2	3
2	3	σ	9	7	6	1	5	2	8	0	4
3	1	4	σ	0	8	7	2	6	3	9	5
4	0	2	5	σ	1	9	8	3	7	4	6
5	5	1	3	6	σ	2	0	9	4	8	7
6	9	6	2	4	7	σ	3	1	0	5	8
7	6	0	7	3	5	8	σ	4	2	1	9
8	2	7	1	8	4	6	9	σ	5	3	0
9	4	3	8	2	9	5	7	0	σ	6	1
σ	8	9	0	1	2	3	4	5	6	7	σ

Fig. 2.3.

For example, the CI-quasigroup whose Cayley table is given in Figure 2.3 is completely determined by the statements that $n = 11$ and that $0 \circ 9 = \sigma$, $0 \circ 0 = 7$, $0 \circ 1 = 5$ and $0 \circ 2 = 4$. This quasigroup is isomorphic to that described in Example 2.2 and can be obtained from it by the mapping

$$\phi = \begin{pmatrix} e & c & c^2 & c^4 & c^8 & c^5 & c^{10} & c^9 & c^7 & c^3 & c^6 \\ \sigma & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{pmatrix}.$$

III. APPLICATIONS TO CRYPTOGRAPHY.

In this section, we show first that a CI-quasigroup provides a means of applying directly J. H. Ellis's original schema for (what he called) a public key encryption system in which the receiver takes part in the encryption process. See J. H. Ellis[6] and [7].

Note. A few years later, the same idea was propounded by W. Diffie and M. E. Hellman in [5]. Their work was probably independent of that of Ellis because Ellis was prevented by the Official Secrets Act from publishing his ideas or any of their proposed subsequent implementations descibed in [7]. On the other hand, the paper of Diffie and Hellman and the subsequent practical implementations of it are very well known.

For convenience, we reproduce the relevant part of [7] as follows:

> "9. Suppose the recipient has two tables M1 and M3 while the sender has one, M2. These machine tables are not secret and may be supposed to be possessed by the interceptor. M1 takes an input k and produces an output x. M2 takes inputs x and p giving an ouput z. M3 takes inputs z and k. All these quantities are large numbers of the same magnitude. We can think of M1 as a linear table or simple list, while M2 and M3 are square tables.
>
> 10. In operation, p is the message which is to be sent and k is a random number, the key, chosen by the recipient. He enciphers k by M1 to get x which he sends. The sender uses x to encipher p with M2 to get z, the

> cipher text, which he sends back. Now the recipient uses k to decipher z by means of M3. It is clearly possible for the entries of M3 to give p under these circumstances, so we have achieved our objective.
>
> 11. If the numbers are large enough and M1 and M2 sufficiently random to avoid working backwards, p cannot be found without knowing k. In public key encryption terms, x is the public encipherment key and k the private decipherment key."

Let (Q, o) be a CI-quasigroup with a long inverse cycle $(c\ c'\ c'' \ldots c^{(t-1)})$ of length t and suppose that both the sender S and the receiver R are provided with apparatus which will compute $a o b$ for any given $a, b \in Q$. The latin square representing this quasigroup acts as the look-up tables M2 and M3 and the long inverse cycle of the quasigroup serves as the third look-up table M1.

The receiver R selects randomly one element $c^{(u)} \in Q$ of the long inverse cycle and uses it to obtain $c^{(u)}J^{-1} = c^{(u-1)}$ which he sends to S who has a message $m \in Q$ which he wishes to transmit to R. S uses $c^{(u-1)}$ to encipher m as $c^{(u-1)} o m$ which he sends back to R. Now R uses c^u to decipher $c^{(u-1)} o m$ as $(c^{(u-1)} o m) o c^u = m$.

Here, $c^{(u-1)}$ is the public encipherment key, c^u is the private decipherment key.

In fact, the system described by Ellis is not a public key encryption system as presently undersstood because a new key k is chosen for each new message (or part message) which is to be sent.

For a present-day public key implementation of the idea, it would be necessary to keep secret the algorithm for obtaining the right crossed inverse of each element of Q. Then implementation might be carried out as follows:

A key distributing centre would be established. Each user would have a computer or a chip card programmed to calculate $v o w$ for every pair $v, w \in Q$. Only the key distributing centre would have knowledge of the long inverse cycle and would use it to distribute a public key $c_i^{(u)}$ and a private key $c_i^{(u+1)}$ to each user U_i. When user U_i wished to send a message m to user U_j, he would send $c_j^{(u)} o m$ which U_j could decipher using his private key $c_j^{(u+1)}$.

However, this scheme is not very secure unless a mechanism is set up by which the CI-quasigroup (Q, o) is changed fairly frequently. The system is more effective if implemented as a one-time pad which is in effect what Ellis was describing. For example, it might be used (i) for sending a message $m = m_1 m_2 \ldots m_r$ in which each portion of the message has its own enciphering and deciphering keys; or (ii) for key exchange without the intervention of a key distributing centre in the following way:

The sender S selects arbitrarily (using a physical random number generator) an element $c^{(u)}$ of the CI-quasigroup (Q, o) and sends both $c^{(u)}$ and the enciphered key or message $c^{(u)} o m$. The receiver R uses his knowledge of the algorithm for obtaining $c^{(u+1)}$ from $c^{(u)}$ (as given in Theorem 2.1, for example) and hence he computes $(c^{(u)} o m) o c^{(u+1)} = m$.

Some further cryptographic applications of CI-quasigroups are considered in a forthcoming survey paper [4] but the readers of this paper may well think of their own.

In the final section of this paper, we explain in more detail how a CI-quasigroup with a specified long inverse cycle may be constructed and stored economically in a computer.

IV. CONSTRUCTION AND STORAGE.

We choose a large prime p such that $p+1$ has a divisor r for which $(-r)^3$ is a primitive root of p (see below) and use it to construct a CI-quasigroup (Q, o) of order p on the set $Q = \{0, 1, \dots , p-1\}$ with an inverse cycle of length $p-1$ in the way described in Theorem 2.1 so that the long inverse cycle is $(0\ 1\ \dots\ p-2)$ and so that $p-1 = \sigma$. (Q, o) is completely defined by the entries of the first row of its Cayley table, so let us suppose that $0oi = h_i$ for $i = 0, 1, \dots , p-1$ and that $h_z = \sigma$, where $0 \leq z \leq p-1$. We store the elements h_i, $i = 0, 1, \dots , p-1$ in the computers of those persons who are to use the system for secure communication.

Note. As already shown, the elements h_i are not independent: $0oi = h_i$ implies $0o(1-h_i) = i-h_i$ and $0o(h_i-i+1) = 1-i$. Also, $h_{p-1} = 1-z$, since $0oz = \sigma \Rightarrow z = \sigma o1 \Rightarrow zo\sigma = 1 \Rightarrow 0o\sigma = 1-z$.

For the purposes of communication, we carry out a random permutation $\alpha: i \to a_i$ of Q (for $i = 0, 1, \dots , p-1$) so as to construct a long inverse cycle $(a_0\ a_1\ \dots\ a_{p-2})$ and a self-inverse element a_{p-1}. (In effect, we are replacing the constructed CI-quasigroup (Q, o) by a CI-quasigroup $(Q, *)$ isomorphic to it .)

To transmit a message a_m ($\neq a_{p-1}$) to a receiver R, we use the computer to obtain $a_{t-1} * a_m$, where a_{t-1} ($\neq a_{p-1}$) is the public key supplied by the receiver R, and send it back to R. On receipt of the encoded message, R uses his computer to calculate $(a_{t-1} * a_m) * a_t = a_m$ as described in the previous section. It remains to explain how to programme the computer and how to select the prime p.

A. *Programming the computer (or chip card)to calculate $a_u * a_v$.*

(i) If $u \neq p-1$, the computer replaces a_u by u and a_v by v and computes uov as follows: From the stored information, $0o(v-u) = h_{v-u}$, whence

$$\begin{aligned} uov &= h_{v-u}+u \text{ if } h_{v-u} \neq \sigma \text{ (that is, if } v-u \neq z \bmod p-1) \\ &= h_{v-u} \text{ if } h_{v-u} = \sigma, \text{ since (in both cases) } 0J^u o(v-u\,)J^u = h_{v-u}J^u. \end{aligned}$$

Suppose that $uov = w \neq p-1$. Then, $a_u * a_v = a_w$.
Suppose that $uov = p-1$. Then, $a_u * a_v = a_{p-1}$ (the self-inverse element).

(ii) If $u = p-1$, the computer replaces a_u by σ and a_v by v and computes σov as follows: From the stored information, $0oz = \sigma$. So, $z = \sigma o1$, whence $\sigma ov = z+v-1$ (since $\sigma o1 = z \Rightarrow \sigma J^{v-1} o 1 J^{v-1} = zJ^{v-1}$.) Thus, $a_{p-1} * a_v = a_{z+v-1}$.

Note. It is never necessary to compute $uo\sigma$ because neither a_m nor a_t is chosen to be a_{p-1}.

B. *Selecting the prime p.*

We may choose a large prime $p \equiv 2 \bmod 3$. Then $p \equiv -1 \bmod 6$ so $p = 6k-1$ say and $p-1 = 6k-2$. Since 3 does not divide $6k-2$, $(-r)^3$ has the same order in the multiplicative group of $\mathbf{Z}_p$ as does $-r$, so we require a positive divisor r of $p+1 = 6k$ such that $-r$ is a primitive root of $p = 6k-1$. We may select p so that one of -2, -3, -6 or $-k$ (or a divisor of $-k$) is a primitive root. (Every $p < 1000$ with $p \equiv 2 \bmod 3$ satisfies this requirement, as has been remarked in [8].)

[If $p = 1181$, then $k = 197$ (a prime) and none of -2, -3, -6 or -197 is a primitive root of p, so this choice of p is inadmissible.]

ACKNOWLEDGEMENTS.

The author wishes to thank József Dénes for introducing the problem of constructing CI-quasigroups with long inverse cycles and for pointing out their appplicability to cryptography and his nephew, James Keedwell, for drawing his attention to the internet paper of J .H. Ellis.

REFERENCES.

[1] R. Artzy, On loops with a special property, Proc. Amer. Math. Soc. 6(1955), 448-453.

[2] R. Artzy, Crossed inverse and related loops, Trans. Amer. Math. Soc. 91(1959), 480-492.

[3] V. D. Belousov and B.V. Tzurkan, Crossed inverse quasigroups (CI-quasigroups), Izv. Vyss. Ucebn; Zaved. Matematika 82(1969), 21-27. (In Russian.) Translated as Soviet Math. Izv. VUZ.

[4] J. Dénes and A. D. Keedwell, Applications of non-associative algebraic systems in cryptography, In preparation.

[5] W. Diffie and M. E. Hellman, New directions in cryptography, IEEE Trans. Inform. Theory IT-22(1976), 644-654.

[6] J. H. Ellis, The possibility of secure non-secret digital encryption, CESG Report, January 1970.

[7] J. H. Ellis, The story of non-secret encryption, World Wide Web at http://www.cesg.gov.uk/about/nsecret/home.htm [CESG Public Key Cryptography Papers - Updated 1999].

[8] R. K. Guy, Private communication to the author. July, 1997.

(Received 20/1/99)