Some Applications of Multiple Key Ciphers

Colin Boyd,
British Telecom,
Data Security Laboratory,
1, Cutler Street, Ipswich IP1 1UX, UK.

Abstract

This paper describes an implementation of a cipher system with any number of keys which is a generalisation of the RSA cryptosystem. Three applications of such a cipher system are given. The general properties required for possible alternative implementations are discussed.

1 Introduction

The insight of Diffie and Hellman [6] was that the enciphering and deciphering keys of a cryptosystem need not be the same. Therefore a cryptosystem could have two keys, one of which would remain secret and the other would be made public. This has led to numerous applications such as digital signatures.

The aim in this paper is to investigate some of the consequences of generalising these ideas. We consider doing this in two ways. Firstly the number of keys in the cryptosystem can be increased to three or more. Secondly the different keys can be distributed to sets of users other than a single user or the set of all users.

We start off the paper with some general ideas about multiple-key ciphers and then consider some applications and how they fit in with these ideas. The applications considered in this paper are selective distribution of information to subsets of a group of users, digital signatures with more than one signatory, and electronic voting. There are many other potential applications. The scheme we consider here appears to be useful for applications of a type concerning different groups of interacting users. The

C.G. Guenther (Ed.): Advances in Cryptology - EUROCRYPT '88, LNCS 330, pp. 455-467, 1988.

importance of such applications is discussed together with some examples in [5].

2 Multiple Key Ciphers

We shall explain our concept of a multiple key cipher in terms of a generalisation of the RSA public key scheme [7]. Other implementations are possible and the precise properties of RSA that are used are examined in section 4 of this paper. An important property of RSA that we make use of is its multiplicative property, namely with fixed modulus and any keys k1,k2,

$$E(E(M,k1),k2) = E(M,k1.k2)$$

for any message M. Our construction of a multiple key cipher is as follows.

A modulus m is chosen by the owner of the scheme to be the product of two large primes as in the RSA scheme. The special properties of the primes which are desirable in RSA are also desired here. A number of keys k1,k2,...,kn are then chosen to satisfy the property

$$k_1.k_2...k_n = 1 \bmod \emptyset(m).$$

The $k_1,...k_{n-1}$ may be chosen at random and kn then chosen to satisfy the equation. To encrypt with the key k_i a message M, with $0 < M < m-1$, is transformed by

$$E(M,k_i) = M^{**}k_i \bmod m.$$

Then it follows that

$$E(E(E(M,k_1),k_2)...),k_n) = M^{**}(k_1.k_2...k_n) \bmod m$$

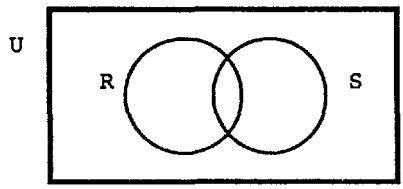
$$= M^{**}(r.\emptyset(n) + 1) \bmod m \text{ for some integer } r,$$

$$= M \quad \text{by Fermat's Little Theorem.}$$

Note that because of the multiplicative property it does not matter in which order the keys are used.

Let U be any population of users of the scheme and K the set of keys $\{k_1,k_2,\ldots,k_n\}$. Any subset of K can be distributed to any subset of U. A message that has been encrypted with a certain number of the keys in K may then be read by a certain subset of U and can only have been written by another subset of U. These subsets are defined by possession of the necessary keys.

For example consider the case where there are only two keys r and s. Let R be the subset of users of the population who possess the key r and S be the set who possess s. These subsets overlap in the subset of users who possess both keys, which may or may not be empty.



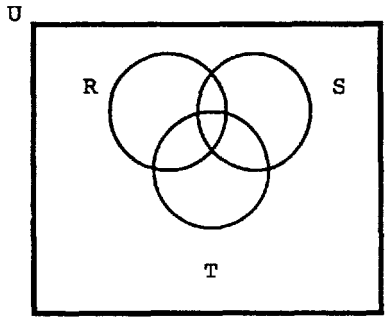
The following table shows the status of the possible messages.

Message	Can be read by	Can be written by
M**r mod m	S	R
M**s mod m	R	S

In the case that R is equal to the whole population U, and S is a single user, we arrive at the familiar situation of the RSA public key cryptosystem. Then messages of the type M**r mod m can be written by anybody but are confidential to the single user, whereas those of the form M**s mod m can be read by anybody but must have been produced by the single user.

When the number of keys is increased to three there are many more possibilities. We extend the previous diagram by adding a third

group of users T in possession of the key t.



The following table shows the status of the possible messages.

Message	Can be read by	Can be written by
M**r mod m	S ∩ T	R
M**s mod m	R ∩ T	S
M**t mod m	S ∩ R	T
M**rs mod m	T	R ∩ S
M**rt mod m	S	R ∩ T
M**st mod m	R	S ∩ T

Where the table indicates that the message can be read or written by S T, it can be written or read by any member of both groups, or, what is just as important, can be written or read by any member of S and any member of T in collaboration. In an application some of the named subsets of U may be empty. In the applications described in this paper we always assume the existence of an authority which is responsible for generating and distributing keys.

3 Applications

3.1 Selective Distribution

This application is concerned with distributing information to one or more selected users out of some user population. There are

various situations where different sets of information may be required to be made available to different sets of entities. Examples are confidential information in companies which is restricted to different departments, and database information which is only available to those groups who have paid for it.

In order to restrict the information only to authorised users the information will be encrypted. The information could be encrypted with a different key for each authorised user or group but this would require many different versions of the information to be held or distributed. Therefore we require that each piece of information is only encrypted with one key but that any combination of the users may be defined for reception of a particular piece of information.

The obvious way to solve this problem is for the authority to issue a key for every possible combination of users. The problem with this is that if there are N users then 2**N-1 keys are required which quickly becomes large as N increases. The solution described here uses the multiple-key cipher and requires only N different keys.

Consider a set-up with three users of a system. The authority chooses three keys r,s and t with

$$r.s.t = 1 \bmod \emptyset(m).$$

Let us call the users A, B and C. These users are then issued with the key sets {r,s}, {r,t}, and {s,t} respectively. The authority can then choose any combination of the users it wishes to distribute a given message M. The way this can be done is illustrated in the following table.

Message	Can be read by
M**r	C
M**s	B
M**t	A
M**rs	B and C

Message	Can be read by
M**rt	A and C
M**st	A and B

Of course messages to be read by all three users can be sent in the clear.

The above scheme can be extended to any number of users by choosing the same number of keys as there are groups. Suppose there are N users and N keys $k_1, k_2, \ldots k_N$. Each user is distributed all keys except one, so that the i'th user is distinguished by not possessing key k_i. Messages are encrypted by the authority using any combination of the keys, and messages are kept secret from the i'th user by leaving k_i out of the keys used in the encryption.

Note the flexibility of this scheme in regard to members leaving or joining the system. This property is identified in [5] as being of great importance in "group oriented cryptography". Members may be added or removed without the need to change the keys of any other members. The authority will only need to re-calculate its inverse key.

In order for this scheme to work the users must not be able to collude to share keys since the keys of any two users could be used to read every piece of information. If this is likely the keys would need to be distributed by the authority in a tamper-proof form which could not be read by the users, and which could only be used in a fixed protocol.

For example, the tamper proof module could be programmed only to output messages which satisfy a certain redundancy condition when decrypted with the correct key. Messages from the authority will be provided with the redundancy condition before encryption.

A similar problem to that addressed here is discussed by Simmons in [8], where the idea of a tamper resistant module plays an integral part in the solution.

3.2 Double Signatures

The idea of digital signature is now well known. In many commercial applications the signature of more than one person is required on a document. We call a signature requiring more than one key a multisignature. Typical uses for such a multisignature are cheques issued by companies which need to be authorised by two people and contracts which are to be signed by business partners.

Multiple key ciphers can provide a neat solution to this problem. A detailed account of various schemes is given in [1]. In this section we show a solution that fits into the general framework of multiple key ciphers. We restrict ourselves to the case of just two signatories.

Two keys r and s are selected randomly (subject to the condition that they are prime to $\emptyset(m)$) and t is chosen to satisfy

$$r.s.t = 1 \bmod \emptyset(m).$$

The keys r and s are distributed to the authorised signatories and t is made public. In order to sign the message M the first signatory forms the signature

$$S1 = M^{**}r \bmod m$$

and passes it to the second signatory. The second signatory can recover the message using s and t since

$$S1^{**}st \bmod m = M.$$

Furthermore he knows it has been signed by the first signatory. If he is satisfied he forms

$$S2 = S1^{**}s \bmod m$$

$$= M^{**}rs \bmod m$$

and passes it to the recipient. The recipient and any member of the public can verify the signature since

$$S2^{**}t \bmod m = M.$$

In terms of the model described in section 2 we may take U to be the set of all users. The keys r and s are then issued to sets of authorised signatories R and S and the key t is issued to all of U. The following table shows the status of the messages.

Message	Can be read by	Can be written by
S1	S	R
S2	U	$R \cap S$

In [1] it is shown how this idea may be extended so that the two signatories can be any from a group. For example this would allow any two directors from the board of a company to sign a document.

Note, however, that it is not possible to extend this scheme to more than two signatories in the obvious way. This is because every signatory needs to be able to read the partial signature before signing, which is only possible for the first or last signatory. It is shown in [1] how this property can be turned to advantage to implement "blind signatures"([3]).

3.3 A Simple Voting Scheme

Various schemes have been proposed for electronic voting ([2],[4]). This application of multiple key ciphers is a new simple voting scheme. It enables users to verify that their votes have been counted while keeping votes anonymous to all other voters. It has the useful property that there is no interactive behaviour required between the authority and the voters, and also that no secret key is required by the voters. In the form explained here it is only suitable for voting either 'yes' or 'no', but the scheme could be extended to allow any number of answers.

The scheme suffers from the disadvantage that the authority is able to read the vote of any person, if it also acts as the issuer of the 'voting slips'. There appears to be a conflict in

voting schemes, also mentioned in [4], between maintaining the confidentiality of the votes cast and ensuring that no voter votes twice. Trust has to be placed somewhere and in this scheme an independent trusted voting authority is assumed. This is consistent with the way that paper voting schemes usually work.

Three keys r,s,t are involved, of which r is kept secret by the issuing authority and s and t are made public. As usual the authority chooses r,s and t to satisfy

$$r.s.t = 1 \bmod \emptyset(m).$$

Each voter is issued a voting slip V which is a block consisting of two parts. One part is a random number q which is used to ensure that the slip is not used more than once, and the other is a component of redundancy which is used to avoid forgery. The redundancy could consist, for example, of every other bit of q being fixed. (The redundancy component can be changed for each election, thus allowing the same keys to be used on many different occasions.)

The voting slip is issued to the voter as V**r mod m. (This must be transported secretly to the correct voter, a problem we do not address here!) If the voter wants to vote 'yes' he forms

$$(V^{**}r)^{**}s \bmod m$$

and sends it to the ballot. Similarly if he wants to vote 'no' he sends

$$(V^{**}r)^{**}t \bmod m.$$

The authority can then validate and count each vote V' by forming

$$V'^{**}t \bmod m$$

or

$$V'^{**}s \bmod m$$

and checking for the redundancy condition. The claimed value of the vote can be sent with it in order to reduce processing.

Voting slips may not be forged since they are signed by the issuing authority. On the other hand they are anonymous (except to the issuing authority) since the voting keys are public. In terms of the model of section two a valid vote must have been written by the issuing authority plus any user, and can be read by any user.

If the same random number is found more than once then all votes with that number should be discarded. (Of course, there is a small probability, depending on the number of voters and the size of m, that a valid vote is discarded.) Copies of all the votes (including any discarded ones) can be published with the results of the ballot and each voter can confirm that his vote was included.

4 Abstraction : Multiple Key Ciphers as Groups

For concreteness we have looked at multiple key ciphers as generalisations of the RSA cryptosystem. In this section we try to abstract the essential properties of RSA that we have used and discuss what could be a more general approach.

We start off from a finite message space M and consider our cryptosystem as a finite set of keys K which are permutations of M. That is each k in K is a map M -> M which is one-to-one and onto (a bijection). We have found a need for the following properties.

Closure Property

Any two keys k and j in K may be concatenated so that k o j is another key in K.

Inverse Property

Each key k in K has an inverse k^{-1} in K such that

$$k \circ k^{-1} = id : M \to M.$$

Associative Property

For any three keys j,k,l in K, we have

$$j \circ (k \circ l) = (j \circ k) \circ l.$$

Commutative property

For any two keys k and j in K, we have

$$k \circ j = j \circ k.$$

We have used these properties to enable us to construct key sets for a multiple key cipher as follows.

First choose any keys in K then concatenate them. The number of keys chosen is not limited and depends on the application.

i) By the associative property the result of the concatenation does not depend on the order in which it is performed.

ii) By the Closure Property the concatenated values give a valid key k in K.

iii) The complementary key of k exists by the Inverse Property.

iv) The commutative property is required because it should not matter in which order the keys are used.

These properties are exactly those that are required to define K as an Abelian Group. The inverse property is common to all invertible cryptosystems including block ciphers such as DES. The closure property, however, is not normally held by a symmetric block cipher but it is held by RSA. The associative and commutative properties are held in our extension of RSA.

In the case of our RSA extension the message space M consists of the integers less than the RSA modulus, and the key group consists of the multiplicative group of integers Z_n^*.

One property of RSA that we have used but not mentioned yet is the trapdoor property. This allows the 'owner' of the scheme, or

what we have sometimes called the 'authority' in this paper, to obtain the correct complementary key while preventing unauthorised parties from finding such a key. In the applications considered in this paper the trapdoor property was relied upon, but further applications may be found which will not require it while the properties in section 2, regarding which entities may read or write a message, still apply. This opens up the possibility of different implementations of multiple key ciphers which do not depend on existing public key cryptosystems. One possible example is the field of integers modulo a prime. Users given a single key selected randomly by the authority can have no knowledge of other users keys allocated by the authority which together form a complementary set.

An interesting further development might be to consider the effect of removing various of the group properties. For example, without the commutative property the order of use of keys would have different effects; this could be significant, for example in the double signatures application.

5 Acknowledgements

I would like to thank E.J.Humphreys for many valuable discussions on the topics in this paper and Mark Stirland for pointing out some errors in an earlier version. Acknowledgement is made to the Director of Research and Technology for permission to publish this paper.

6 References

[1] C.A.Boyd, Digital Multisignatures, IMA Conference on Cryptography and Coding, Cirencester, December 1986.

[2] D.L.Chaum, Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms, Comm.ACM, 24,2,(1981), 84-88.

[3] D.L.Chaum, Blind signatures for untraceable payments, Proceedings of Crypto 82, Plenum Press 1983, pp.199-203.

[4] J.D.Cohen & M.J.Fischer, A Robust and Verifiable Cryptographically Secure Election Scheme, Proceedings of IEEE Conference on Foundations of Computer Science, 1985.

[5] Y.Desmedt, Society and Group Oriented Cryptography, Proceedings of Crypto 87.

[6] W.Diffie & M.Hellman, New Directions in Cryptography, IEEE Transactions on Information Theory,IT-22,6,1976.

[7] R.Rivest, A.Shamir & L.Adelman, A method for obtaining digital signatures and public key cryptosystems, Comm.ACM 21,2(1978), 120-126.

[8] G.J.Simmons, How to (selectively) broadcast a secret, Proceedings of IEEE Conference on Security and Privacy 1985.