Project 2 looks more reasonable, maybe because your description of Project 1 is muddled terribly. Talk to me about these today.

C.S. 244
FALL 1974

Ralph Merkle

Project Proposal

Topic: Establishing secure communications between seperate secure sites over insecure communication lines.

Assumptions: No prior arrangements have been made between the two sites, and it is assumed that any information known at either site is known to the enemy. The sites, however, are now secure, and any new information will not be divulged.

Method 1: Guessing. Both sites guess at keywords. These guesses are one-way encrypted, and transmitted to the other site. If both sites should chance to guess at the same keyword, this fact will be discovered when the encrypted versions are compared, and this keyword will then be used to establish a communications link.

Discussion: No, I am not joking. If the keyword space is of size N, then the probability that both sites will guess at a common keyword rapidly approaches one after the number of guesses exceeds sqrt(N). Anyone listening in on the line must examine all N possibilities. In more concrete terms, if the two sites can process 1000 guesses per second, and desire to establish a link in roughly 10 seconds, then they can use a keword space of size $N=10{,}000^2=10^8$. If the enemy is presumed to have a comprable technology, i.e., 1000 guesses/sec, then he can consider all 10^8 possibilities in $10^8/10^3$ seconds, or 10^5 seconds, which is about one day. As the

amount of time which is devoted to establishing the link is increased, and as technology is improved, the two sites get a bigger and bigger advantage over any enemy, for the work done by the enemy increases as the square of the work done by the two sites. Thus, if the two sites are willing to devote 10 times the effort, any enemy must devote 100 times the effort to crack the code. Thus, it is possible to establish a link in 100 seconds that will remain secure for about 100 days. If the technology improves by a factor of 10, then it is possible to establish a link in 10 seconds that will remain secure for 10 days. If both technology and the effort devoted to guessing increase by 10, then it would be possible to establish a link in 100 seconds that would need 1000 days, or 3 years, to break.

Problems: While a very secure link can be established in reasonable time, it is unfortunetly the case that we do not know with whom we have established this link! If we assume that the enemy has the ability to modify the communications we transmit, then he can simply engage in precisely the activity outlined, and thus establish a secure link with both sites, while the sites think they have established a link with each other. Fortunetly, the two sites now posses information that they know must be the same, if no enemy has altered their communications. This is the keyword they have agreed upon. Since the enemy will be unable to control the selection process completely, the two keywords will probably differ. If the enemy used the same set of keywords to establish

the links with both sites, then there is a 1/sqrt(N) chance that the two sites have selected the same keyword. The two sites must now one way encrypt the keywords that they are using for the link, and somehow transmit them over a line which, while not secure, is such that it cannot be tampered with. A radio link might qualify. If threat monitoring is sufficient, the two sites can simply keep records of the encrypted version of the keyword selected, and compare these records at a later date. If the 1/sqrt(N) chance that the two keywords will be the same, but still known to the enemy, is too high, then a complete record of all guesses made by both sites can be kept. Compared at a later date, these records would reveal that three sets of guesses were made by the three elements in the communications link, not two sets of guesses. These guesses could also be transmitted over any available communications link, and checked before message traffic was started. If the enemy is only monitoring the communications link, after he has established himself in it, then it might be possible to slip these facts through the link. If the link is the only method of communication between the two sites, and is such that transmissions might be altered, and if the enemy is alert to the possible transmission of information over the link itself, then it would seem that no method would be fully secure. The link could be undetectably

cracked. This limitation would seem to make the method outlined suitable for use in a distributed, cryptographically secure, network. Each node would have many methods of communicating with other nodes. Once links were established, and confirmed for the first time by special techniques, the network could constantly change its own passwords, without any outside help, and re-establish broken links, and confirm them. The only method of cracking such a net would be to cut off the communications between one node and all other nodes, pretending that the node had crashed, and then follow the normal linkage recovery procedure. This would have to be done at a time when the node in question actually had crashed, so hard that it had no memory of any of its previously established links, and so could be fooled by the enemy into thinking that the enemy computer was the rest of the communications network. This would compromise only messages addressed to or from the node in question, and could be easily detected if even one communication link remained between the node and the rest of the network. Even a fallible human link could be used, and for this purpose would be better than an unmonitored wire. Nodes could use idle time to establish new and harder to break links.

Work to do: The major work to be done involves the statistical analysis of just how secure things are, how long it would take to establish links, what the chances are of not getting a link in a reasonable time. In addition to the straight

statistical work are such questions as: what is the best technique, computationally, to use? A good deal of information is being transmitted over a link, can it be compressed? Can an intelligent terminal be used as half of a link, and how should it be programed? Can two micro computers establish such a link, in spite of the fact that it appears to require a memory big enough to hold all the guesses? Can all this information be compressed into a useful "how to" manual, so that anyone desiring to establish such a link can evaluate the methods and trade-offs intelligently, with little effort? Is this method really worth anything? To who? This does not even touch on the questions involved in the design of a distributed network. In addition, the question of how to fool and confuse an enemy who has broken into, (and is therefore participating in,) a communications link, into passing along information that would allow his presence to be inferred, seems to be both interesting and complicated. Thus, the major result of this quarter project would be written, with perhaps some programs to check out various points of the protocol.

Method 2: Under the same set of assumptions, another method of establishing communications appears, I emphasize appears, to be feasible. This technique would involve the conversion of a normal, two-way encryption technique into an apparently one-way encryption technique, in many small, easy to understand steps. The resulting

encryption algorithm would appear to be an incomprehensible, one-way encryption technique. It would be equivalent, however, to the original two-way technique from which it was derived. The one-way technique would then be transmitted to the other site, which would use it to encrypt messages. The only way of decrypting these messages would be to use the two-way technique, which was retained by the original site. This method would also have advantages in other applications, for example, where there was a risk of capture, and the possibility that any cryptological techniques used at a site would become known to the enemy. If a one-way encryption technique were used, with the original two-way version kept in a safe place, then the one-way version could be distributed to anyone who wanted a copy. I think that such a method would require large amounts of computer time, (many minutes), on a medium scale computer. In addition, I am unsure as to the actual success of such a program. Finally, it would be difficult to demonstrate that such a technique was actually unbreakable, or nearly so, for I am not well trained in the techniques of cryptanalysis, and any demonstration that a complex scheme is foolproof would seem to require such knowledge. P.S. I'm not as convinced as this seems to say that the method won't work

Second Project Proposal:

The use of/data compression method, derived from parsing methods, as a preliminary step in encryption, along with some encryption techniques. At this point, I must confess, that I am not entirely thrilled by the prospect of engaging in this project, and will expand

upon it only if prodded.