CHAPTER 13

How to Insure That Data Acquired to Verify Treaty Compliance Are Trustworthy*

G. J. SIMMONS
Sandia National Laboratories
Albuquerque, New Mexico 87185

*This chapter first appeared in the *Proceedings of the IEEE,* vol. 76, no. 5, May 1988.

Abstract -In a series of papers [6–8] this author has documented the evolution at the Sandia National Laboratories of a solution to the problem of how to make it possible for two mutually distrusting (and presumed deceitful) parties, the host and the monitor, to both trust a data acquisition system whose function it is to inform the monitor, and perhaps third parties, whether the host has or has not violated the terms of a treaty. The even more important question of what dam will adequately show compliance (or noncompliance) and of how this data can be gathered in a way that adequately insures against deception will not be discussed here. We start by assuming that such a data acquisition system exists, and that the opportunities for deception that are the subject of this chapter lie only in the manipulation of the data itself, that is, forgery, modification, retransmission, etc. The national interests of the various participants, host, monitor and third parties, at first appear to be mutually exclusive and irreconcilable, however we will arrive at the conclusion that it is possible to simultaneously satisfy the interests of all parties. The technical device on which this resolution depends is the concatenation of two or more private authentication channels to create a system in which each participant need only trust that part of the whole that he contributed. In the resulting scheme, no part of the data need be kept secret from any participant at any time; no party, nor collusion of fewer than all of the parties can utter an undetectable forgery; no unilateral action on the part of any party can lessen the confidence of the others as to the authenticity of the data and finally third parties, that is, arbiters, can be logically persuaded of the authenticity of data. Thus, finally after nearly two decades of development a complete technical solution is in hand for the problem of trustworthy verification of treaty compliance.

1 INTRODUCTION

The best known example of a treaty verification system is the series of systems developed at the Sandia National Laboratories to monitor compliance by the Russians with a proposed comprehensive nuclear test-ban (CTB) treaty [6-81. Although the data acquisition system (RECOVER) developed to enable the International Atomic Energy Agency (IAEA) in Vienna to remotely monitor the compliance of a worldwide network of power reactors with the terms of their licensing agreements is less well known, it must satisfy precisely the same objectives for the participants as the CTB verification system. There have also been similar systems designed for arms control purposes for the Arms Control and Disarmament Agency (ACDA) and for continuous inventory by the Nuclear Regulatory Commission (NRC) of plutonium during fuel rod reprocessing by commercial facilities, which share many of the same system objectives. In this chapter though, we shall use as the paradigm for such monitors the system for verifying compliance with a CTB treaty, i.e., a treaty banning all underground nuclear weapons testing. Although the problem has been described elsewhere, we repeat the essential points here, primarily to make clear the conflicting interests of the various participants.

2 VERIFICATION OF A COMPREHENSIVE TEST RAN TREATY

For over two decades, the United States and the Soviet Union have explored, and on occasion negotiated, the details of a comprehensive nuclear test-ban treaty as a means to slowing the arms race. The immediate object of a comprehensive test-ban treaty would be to stop *all* testing of nuclear weapons, thereby essentially freezing the weapons technology at its state of development at the time the treaty takes effect, and hence eventually reducing the chance that another round of the arms race might occur based on yet another major improvement in nuclear weapons technology. Test-ban treaties prohibiting surface, ocean, and space testing of nuclear weapons are in effect and have been abided with by both sides in precisely those areas where verification of compliance by what has been euphemistically called “national means” is possible. In other words, the nation doing the monitoring, for our purposes the U.S., is limited to those observations that are possible from its sovereign territory or from the territories of its allies or from space using satellites. The most reliable technique for detecting underground tests, and essentially the only direct measurement method that can be used at a distance, is to measure the ground motions resulting from the underground detonation using seismic sensors. Unfortunately the threshold of yield for seismic detection at teleseismic distances, from the U.S. or from Scandinavia, is high enough that meaningful weapon development could be carried out below the teleseismic detection threshold. Just how small an underground test can be detected is a function of many things, some that are under the control of the tester, such as the geology of the test site, decoupling chambers for the detonation, time of the test, etc., and some that can be jointly agreed to in the terms of the treaty such as how close the monitoring stations can be to known test ranges and of the physical emplacement of the seismic sensors. Since the purpose of a comprehensive test-ban treaty is to slow the arms race by stopping the development (proof testing) of new nuclear weapons technology, such a treaty is logically feasible only if each party can be confident that the other cannot continue clandestine testing, and hence development of new weapons, to gain an advantage over the other. It is generally accepted by nuclear weapons designers that there is a lower limit to the size of the detonations needed to conduct meaningful weapon development programs, for the purpose of argument say one kiloton, and that tests involving yields below this limit are unlikely to have a significant impact for new weapon systems. The bottom line, which has been recognized by both sides in the negotiations, is that unlike previous treaties in which national means of verification were available, and adequate, that verification of compliance with a comprehensive test-ban treaty would necessitate emplacing seismic monitoring stations within the sovereign borders of the country being monitored (the host) and/or his allies. This would require a radical departure from previous treaty protocols since it would be necessary for the host to cooperate to make it possible for the monitor to verify compliance with the terms of the treaty. Protocols of this sort, anticipated in the verification means for the comprehensive test-ban treaty discussed here and in the SALT II (Strategic Arms Limitation Treaty) where each side would have had to cooperate in order for the other to verify the number of launch vehicles fielded, are apparently about to be realized for the first time in the intermediate-range nuclear forces (INF) treaty between the United States and Russia that has just been signed. With suitable placement of the sensors, seismic techniques that the U.S. has proven by monitoring underground tests at the Nevada Test Site to be capable of detecting subsurface tests and of discriminating the signals from naturally occurring seismic background, are available so that either nation could be extremely confident that no meaningful violations of the treaty could go undetected. Consequently, if it were possible to have appropriately sited seismic monitoring stations within the host's territory manned by the monitoring country's personnel a proven means of verifying compliance with an underground test-ban treaty exists. The difficulty, however, is that continuously manned installations are unacceptable.

A problem that the Sandia National Laboratories has worked on for over two decades has been to develop an unmanned seismic monitoring system, Figs. 1 and 2, that could satisfy the national interests of all parties. It is not difficult to physically secure the seismic sensor package in subsurface emplacements as shown in Fig. 2 since the seismic sensors themselves would detect any attempt to gain physical access to them long before they were in jeopardy. Hence only the data stream sent through an open communications channel would be subject to possible manipulation. From the viewpoint of the monitor, an opponent, usually assumed to be the host for the sensor emplacement, but possibly a third party desiring to undermine the treaty, may either introduce fraudulent or altered messages. For example, the host, if he can do so without being detected, may wish to substitute innocuous seismic records in the stead of incriminating ones that would reveal that tests had been conducted in violation of the terms of the treaty, thus lulling the monitor into erroneously believing that the treaty was being abided with. Conversely, he may wish instead to introduce spurious incriminating messages indicating that tests have occurred when in fact none have been carried out thereby misleading the monitor into erroneously reporting nonexistent violations. This latter stratagem is especially significant when only a limited number of on-site verification inspections are permitted the monitor.*

*Note added in proof: To provide information required for more reliable monitoring of underground nuclear detonations, the U.S. on August 17, 1988, conducted an underground nuclear weapons test at the Nevada test site monitored and instrumented on site by Soviet scientists. The USSR reciprocated on September 14, 1988, with a test shot at their Semipalatinsk test site monitored on site by U.S. scientists.

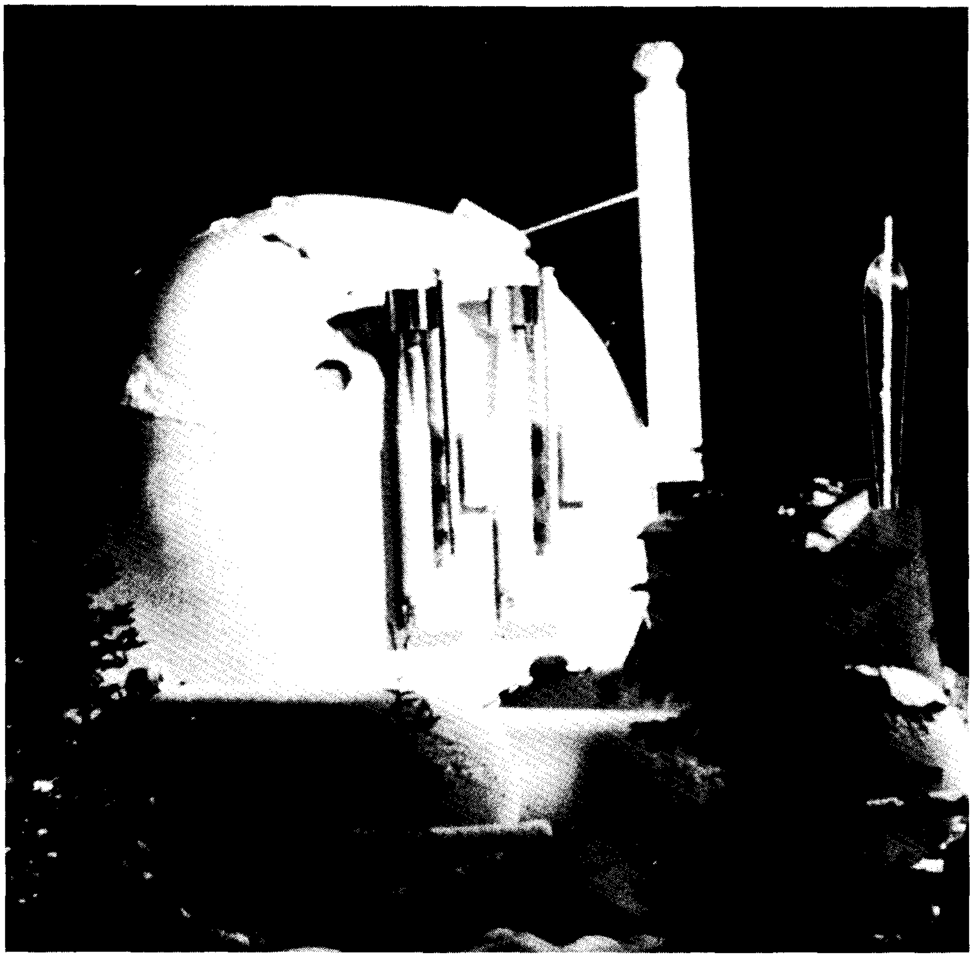

Figure 1 Prototype seismic monitoring station for verification of CTB (Alaskan installatlon). Reprinted with permission from Sandia National Laboratories.

Therefore, in order for a system to be acceptable to the U.S. it must be very improbable that anyone, either the Russians or a third party, could utter an undetectable forgery, that is, the messages must be capable of being authenticated (by the U.S.) as having originated with the seismic sensors that the U.S. had emplaced, and also that the data have not subsequently been tampered with. If only the U.S. objective had to be met, this would be an easy problem to solve. A conventional, that is, single-key, cryptosystem could be emplaced by the U.S. along with the seismic sensors in the borehole, and as in military communications systems a known authenticator appended prior to either block or cipher feedback stream encryption.* The resulting data stream (cipher)

*The reader is referred to the chapter "A Survey of Information Authentication" by G. J. Simmons in this volume for a more complete discussion of the standard military authentication protocol.

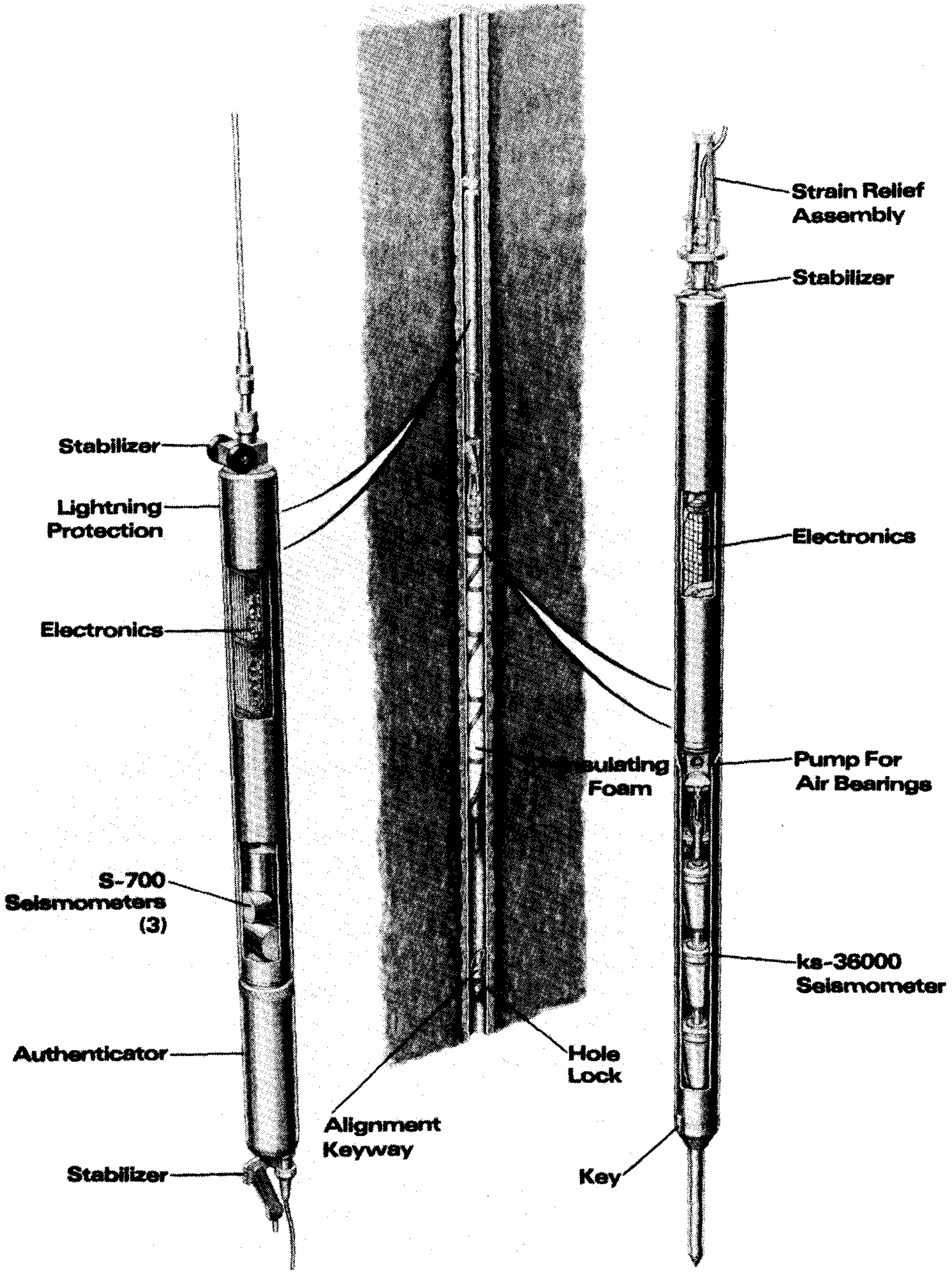

Figure 2. Downhole seismometer package. Reprinted with permission from Sandia National laboratories.

would, of course, be inscrutable to the Russians, but easily authenticated by the U.S. Such a system, however, would be totally unacceptable to the Russians for sound logical reasons. Each seismic station gathers approximately 10^8 bits of data each day, and as presently envisioned these data would be communicated by satellite relay in either real time or near real time to receivers in the continental U.S. The Russians might suspect that this communications channel was being used to communicate data other than that agreed to in the test-ban treaty. Since in conventional single-key cryptography, if one has the decrypt key to enable him to decrypt ciphers, he also has the ability to encrypt, that is, the ability to utter fraudulent ciphers, it is not possible in a single-key cryptosystem to give the Russians the capability to verify in real time that nothing other than what was agreed to by treaty is being communicated. One possibility would be for the monitor to change keys with each transmission, that is, to **use** what are known as session keys, and to give the Russians the key used in a session immediately after the cipher was received and authenticated by the U.S., so that they (the Russians) could verify that the previous cipher decrypted to the proper text, which they would know either from their own corroborating seismic sensors and/or from receipt of an unencrypted version of the message from the monitor's sensors. Unfortunately (and unacceptably), in view of the high data rate, for any practical keying period this requires the host to trust the monitor with too many bits of information before he can verify that nothing has been concealed in the transmission. Of course the host could refuse to cooperate for future transmissions if he detected deception by the monitor, but depending on the time and nature of the transmission the damage could already have been done.

3 VERIFICATION WITHOUT SECRECY

It was at this point that studies of "message authentication without secrecy" were begun at the Sandia Laboratories in the early 1970s. The problem as it was viewed at that time was to find a means for authenticating digital messages* without requiring secrecy for the message itself [7,10]. Recall that the first discussion of two-key (read also public key) cryptography in the open literature [3] appeared several years later (1976) so that the only tool available for a system that was to be shared with the Russians at that time was conventional single-key cryptographic techniques, applied so as to approximate the desired **end** result of authentication (to the monitor) without secrecy (to the host). The compromise solution, found by Simmons, Stewart, and Stokes in 1974 [10], was to form an authenticator that was much shorter than the message, where the authenticator was made to be a function of the entire message through a hashing type function. This authenticator was then block encrypted and appended to the unencrypted message. Today this appended authenticator would be called a MAC or message authenticating code. This solved the problem of making it possible for the host to monitor messages in real time as they were transmitted; however, the appended (encrypted) authenticator was still inscrutable until he was later given the key with which it had been encrypted. Ironically, the host and monitor could each trust this system to the same level of confidence for the same reason. The monitor trusts the authentication

*The terms message and data are used interchangeably in this chapter since there is no chance of confusion; however, the reader should be aware that the term "message" normally means the authenticated information or data, not the raw data itself.

since to create a forgery the host would have to invert from a known plaintext/cipher pair, that is, break the cryptosystem by cryptanalysis, to find the key used by the monitor. On the other hand, the host is satisfied that the monitor did not conceal information in the preceding transmission if the key he is given generates the authenticator that was transmitted since in order to conceal information in the authenticator the monitor would have had to solve for the (unique?) key relating the plaintext and the desired bogus authenticator; that is, to have solved precisely the same problem on which the host bases his confidence in the authenticator.

To shorten the periods of implicit trust required of the host, smaller blocks of information can be authenticated, at the expense of having to have a unique session key for the encryption of each block. However, keys can be generated sequentially by the same cryptoalgorithm used to encrypt the authenticator, so that for all intents there are an unlimited number of session keys available. This makes it feasible to process shorter blocks of data using a unique session key for each block, with a flow of session keys being made available to the Russians after essentially only the delay of a two-way satellite relay link. In the limit, with block size and the two-way delay, such a scheme approximates very well a true message authentication without secrecy system.

The second iteration in the evolution of treaty verification systems was made shortly after Diffie and Hellman proposed public key cryptosystems in 1976 [3]. Two-key cryptography provided a ready-made solution to the problem of message authentication without secrecy, since the fundamental attribute of two-key cryptography is the separation of the secrecy channel from the authentication channel; both of which are inextricably linked in single-key cryptosystems. In two-key cryptography, the encrypt and decrypt keys are not only different, but it is also computationally infeasible to determine at least one of the keys from a knowledge of the other key, even with arbitrarily many matched plaintext message/cipher pairs. If the receiver (decrypt) key cannot be deduced from a knowledge of the transmitter (encrypt) key, then the transmitter key may be publicly exposed, so long as the receiver key is kept secret, without jeopardizing the transmitter's ability to communicate in secret to the receiver, although the receiver cannot authenticate the source of the communication, that is, cannot be sure of the origin of the ciphers he receives. This is the secrecy channel. Conversely, if the transmitter's encrypt key cannot be recovered from a knowledge of the receiver's decrypt key, etc., then, although secrecy is impossible, the receiver can be confident that the communication originated with the purported transmitter and that the message has not been altered in transit to the same level of confidence that the transmitter can be relied on to keep the encrypt key secret. This is the authentication channel.

Given the availability of an authentication channel an obvious solution to the authentication without secrecy problem would be for the U.S. to install the (secret) authentication function along with the seismic sensor package in the borehole. The downhole package would also be equipped with a variety of sensors designed to detect any attempt to tamper with the package or with the information processing subsystem and to volatilize the secret keying variable if tampering is detected. The decrypt key would be shared with the Russians and perhaps with third parties or arbiters such as the United Nations, etc. The messages would consist of the seismic data along with agreed-on identifiers, station ID number, date, clock, message number, etc., that are required, not only for their obvious utility, but also to provide the redundant information needed by the U.S. to authenticate the messages. This redundant information would of course be known in advance by the Russians so that there would be no possibility of hiding covert communications in what was claimed to be simply an overt authenticator. The

Russians could decrypt the transmission in real time, perhaps even delaying the transmission in a data buffer for the time required to decrypt it, to satisfy themselves that nothing other than the agreed upon seismic data and prearranged formatting information were present. Thus no part of the transmission would need to be kept secret from the Russians at any time. Similarly, the U.S. would decrypt the cipher on receipt and accept the transmission as authentic if and only if the expected redundant formatting information or the deliberately introduced (but publicly known) authenticating information was present. This scheme depends only on the availability of an authentication channel, separate from the secrecy channel, and hence is not dependent on any particular two-key cryptoalgorithm. At the Sandia National Laboratories, however, we have chosen to use the Rivest-Shamir-Adleman (RSA) cryptoalgorithm [4]. The interested reader is referred to either the chapter "Contemporary Cryptology: An Introduction" by J. L. Massey appearing in this volume or to any of several references [2, 91 for a detailed discussion of the application of the RSA cryptoalgorithm to message authentication. We describe only the bare essentials here, since it will be necessary to refer to some of the associated parameters in subsequent sections.

In the RSA system, the user chooses a pair of primes p and q so large that factoring n = pq is beyond all projected computational capabilities. p and q are kept secret. He also chooses a pair of numbers e and d, where $(e, \phi(n)) \equiv 1$ and $ed \equiv 1 \bmod \phi(n)$; $\phi(n) = (p - 1)(q - 1)$.* In other words, e and d are multiplicative inverses in the group of residue classes modulo $\phi(n)$. As already mentioned, for an authentication channel, the encrypt key e is kept secret, while the decrypt key d and the modulus, n, may be publicly exposed.

A message $m <$ n is encrypted in this system to the cipher c by the transmitter, using the encrypt key (e, n), by the rule

$$m^e \equiv (\bmod\ n)$$

and c is decrypted by the authorized receiver, using the decrypt key $(d,$ n), by the rule

$$c^d \equiv (\bmod\ n)$$

Authentication, as we have already pointed out, is based on the receiver finding information already known to him in the decrypted cipher. For example,

$$\begin{aligned} \text{if } p &= 36756001033 \\ \text{and } q &= 110411555503 \\ \text{so that the modulus } n = pq &= 4058287248123404834599 \\ \text{and } \phi(n) &= 4058287247976237278064, \\ \text{then for the encrypt key } e &= 1897225149044257283231 \\ \text{the matching decrypt key } d &= 15551. \end{aligned}$$

Using these cryptovariables, the message 1234567890 with the authenticator SANDIA,

$$m = 1234567890\text{SANDIA} = 1234567890291124141911$$

*$\phi(x)$ is the Euler phi function of x (x, a positive integer) and is simply the number of positive integers less than x that have no factor other than 1 in common with x.

would encrypt to the cipher

$$c \equiv m^e \equiv 17685765650131926077\!10 \pmod{405828724812340483459\!9}$$

while c would decrypt to recover the message

$$m \equiv c^d \equiv c^{15551} \equiv 1234567890\text{SANDIA} \pmod{4058287248123404834599}$$

The appended authenticator SANDIA has been encoded and decoded by the simple numeric substitution: $A = 11$, $B = 12$, $\cdots$, etc. In this example, only ciphers that decrypt to numbers ending in $\cdots 291124141911$, that is, to the encoding of SANDIA, would be accepted as authentic transmissions. The probability that a randomly chosen cipher would be accepted as authentic in this case is $\approx 3 \times 10^{-9}$ or one chance out of 26^6.

The cryptosecurity of the RSA system is based on the difficulty (infeasibility?) of factoring suitably constructed and sufficiently large composite moduli, n. Obviously, if an opponent can factor n to recover p and q, he can then calculate the multiplicative inverse e of d using the Euclidean algorithm just as the user did to set up the system and hence be able to encrypt, that is, to authenticate, messages. Since computing the multiplicative inverse e of d from a knowledge of only d and n is essentially the same as factoring n or determining $\phi(n)$, e is as secure as factoring n is difficult. Therefore, so long as the factors p and q, and the encrypt key e are kept secret, the authentication channel based on the RSA system is thought to be as secure as factoring, which with reasonable conditions imposed on the choices for p and q is now generally accepted to be a computationally infeasible problem.

In the most direct application of the RSA-based authentication channel to insuring the trustworthiness of the seismic data acquired to verify compliance with a comprehensive test-ban treaty, the U.S. would choose the primes p and q and one of the exponents e or d and then calculate the inverse exponent (d or e, respectively) using the Euclidean algorithm. As part of the initialization procedure by the U.S., n = pq and e would be securely entered into the downhole seismic package. The decryption key d and n would be given to the Russians and perhaps to third parties, and of course retained by the U.S. In operation, the seismic data as well as the redundant identifying information would be block-chain encrypted by the downhole package using the secret encrypt key e and the publicly known modulus n. The host can now satisfy himself that there is no covert communication by decrypting the cipher and verifying that only the previously agreed upon redundant information and the seismic data are present. Recall that he is assumed to know the actual seismic data (message) either from his own sensors or from data links to the monitor's sensors placed ahead of the authentication operation. The monitor, on the other hand, can be certain of the authenticity of a message (containing message numbers, clock readout, etc.) since by hypothesis neither the host nor any third party can compute e from the exposed n and d. Thus the host need not trust the monitor at all, while the monitor is free to introduce as much redundant (but prearranged with the host) information as required to provide authentication confidence.

4 VERIFICATION WITH ARBITRATION

Unfortunately, although the system just described allows the monitor to authenticate messages to whatever level of confidence he desires while at the same time permitting the host to reassure himself that no unauthorized information is concealed, it leaves unanswered another problem that could defeat the purpose of a treaty verification system. If unilateral response by the monitor, such as abrogation of a treaty or resumption of atmospheric testing of nuclear weapons as the U.S. did in 1962 in response to the Soviet's 1961 violation of the Joint Understanding of a moratorium on such tests, is the only action to result from a detection by the monitor of a violation of the agreement, the system **just** described suffices. If, however, the action to be taken by the monitor in the event that a violation is detected involves convincing third parties or arbiters, such as the United Nations, NATO, etc., then it must be impossible for the monitor to forge messages. Otherwise, the host could disavow an incriminating message as being a forgery fabricated by the monitor, an assertion that the monitor could not disprove if he has the known ability to encrypt messages and hence to create undetectable forgeries.

In 1980, research at Sandia was redirected to solving the authentication with arbitration problem and the related problem of preventing unilateral actions by the host from making it impossible for the monitor to prove the authenticity of a message. For arbitration to be possible, it clearly must be the case that neither party (host or monitor) is in possession of, nor capable of calculating **by** any feasible amount of computation, the encryption exponent e, since they could then utter undetectable forgeries. As long as this possibility exists it is impossible for the monitor to logically compel a third party to accept the authenticity of a message. There are a class of unconditionally secure authentication schemes that permit arbitration of transmitter/receiver (host/monitor) disputes* that depend on the availability of an arbiter that both parties unconditionally **trust.** Unfortunately, there is no arbiter who is unconditionally trusted by both the U.S. and Russia, so we must settle for only computationally secure authentication with arbitration schemes. Various schemes were considered in which the host and the monitor each contributed to the key in **such** a way that the result was unknown to both. Since there are no scenarios in which the objectives of the monitor and of the host are both furthered by their collaborating to create forgeries that would be accepted as authentic by third parties, this joint generation of key at first appears plausible. For example, they might each enter (in secret from all other participants) in the downhole data processing package a binary crytographic key and the exclusive-OR of the two keys could be used as the secret key e. In effect, the actual key ***e*** would be the Vernam encryption of each parties' key with the unknown (one-time) key of the other party which, as is well known, insures that the result is mathematically demonstrably cryptosecure to each party. In other words, for randomly chosen input keys neither the host nor the monitor could infer anything about ***e*** from their knowledge of the random component they had selected, hence neither is capable of uttering an undetectable forgery. The host, however, could still cheat in the following way. He could test with impunity, and when incriminating records were exhibited by the monitor, claim that his contribution to the key had been compromised; i.e., that one of his people had defected, his files had been rifled, etc. In fact, if he is brazen enough, he could simply publish some number that he claims to have been his contribution and thereby destroy the ability of the monitor to

*The reader is referred to the chapter "A Survey of Information Authentication" by G. J. Simmons in this volume for a description of unconditionally secure arbitration codes that permit arbitration.

prove the authenticity of any messages. If the published number is not the correct one, the monitor, using his contribution to the key, could verify that the released number was bogus, but would not be able to prove this to anyone, since they could not be convinced that the monitor was telling the truth about his number. The point is that in such a scheme the host can unilaterally make it possible for the monitor to generate undetectable forgeries, and hence make it impossible for the monitor to prove to an unbiased third party that he did not do so.

Therefore, a solution to the authentication with arbitration problem must both make it possible for the monitor to logically compel **third** parties to accept the authenticity of messages and make it extremely improbable that the host can by any unilateral action lessen the monitor's ability to convince third parties. The solution to these problems which constituted the third iteration of treaty verification systems [7] was to have the downhole equipment nondeterministically generate p and q in secret from all parties and then select an e (again nondeterministically and in secret from all parties). Only n and d, which is calculated using the secret values of p, q, and e, are revealed. We have mentioned the need for selecting "good" primes, the most obvious condition being the magnitude of the numbers, but also such that $p - 1$ and $q - 1$ have large prime factors, etc. All of these criteria can be programmed in, along with a nondeterminate random number generator that provides an unknown seed to start the prime generation process. For example, if a **100-bit** seed is needed, a random process such as radioactive decay, could be observed for 100 intervals of sufficient length that many decays would occur in each interval. At the end of each interval a 0 or 1 is entered in the corresponding bit position according to whether an even or odd number of particles had been counted. Using the resulting random seed, the next larger "good" prime would be found and used as p or q. e could be generated in a similar manner and d calculated using the Euclidean algorithm. The decryption key n and d would be output at the end of the initialization process to the monitor, the host and to any arbiters needed. In such a system only the downhole equipment could generate authentic messages, and unlike the earlier systems, all of the objectives described thus far for each of the parties are realized.

1. No party can forge messages that would be accepted as authentic.
2. No part of the message is concealed from the host, or from specified third parties.
3. The host, the monitor, and third parties are all able to independently verify the authenticity of messages.
4. No unilateral action by any of the participants can lessen the confidence of any other party as to the authenticity of messages.

5 VERIFICATION IN THE PRESENCE OF DECEIT

For a time it was thought that the system just described had solved the treaty verification problem [7]. In principle, that is, so far as information security was concerned, this was true. Unfortunately, it is not true in practice, not because of any logical flaw in the system, but rather because of the practical impossibility of realizing the required properties in a mutually convincing way. We have discussed at length how either the host or the monitor, if they can learn the encryption key, can create forgeries to their benefit and to the detriment of the other party. It is not even necessary that the key be directly compromised, but only that it be a computationally feasible task to recover it from the information that is exposed. Consequently, the party that builds the downhole equipment potentially has an enormous, probably insurmountable, advantage over the other. Recognizing this, several protocols of the "take any card" sort were devised in which the party making the equipment would provide several sets of equipment, one of which would be selected by the other party and installed in the borehole under joint control and the others of which could be operated or dissected by the other party to convince themselves that they all operated exactly as they should. One of the problems with all such schemes is whether there exists any random number generator that can be convincingly shown to be nondeterministic by observing the output. A good case in point are maximal period n stage linear feedback shift registers whose output sequences satisfy most tests for randomness, but whose future output can be completely predicted with polynomial (in n) difficulty after only 2n bits of the output are observed, using Berlekamp's algorithm [1]. The point is that it is a much easier task to exploit a known bias than to detect an unknown one. Because of this, neither party is apt to trust a key generator built by the other. Intricate schemes were considered to get around this problem by having the parties share in the key generation process, the simplest of which is merely the downhole equivalent of the exclusive-OR technique discussed earlier. In this proposal the Russian sequence generator, representing their interests, would present n bits of equivocation to the U.S. and vice versa. In fact, there is nothing logically wrong with this approach to jointly generating a key that presents n bits of uncertainty to each party. The problem that is not solved by this scheme is that this key, once generated, must be used in a piece of cryptoequipment built by one of the participants. As anyone who has ever struggled with the Tempest certification of electronic equipment knows, it is difficult to the point of impossibility to be certain that all of the "sneak" channels for leaking information have been plugged and for the present application the problem is much worse. The natural suspicion of the party who did not build the equipment is that the one who did will have deliberately introduced time jitter, crosstalk, amplitude modulation or some other form of leakage for keying information, which can be made to be arbitrarily difficult to detect unless one knows the nature of the leak. The conclusion was that this problem could only be solved if each of the parties had an opportunity to process the signal in equipment that they supplied before the cipher was sent up the borehole. Furthermore, jointly generated keys were ruled out, since whoever's equipment operated last on the data could conceivably telegraph the key by subtle modulation. Thus each party's equipment operates only on and with information known to him. In the resulting system, the U.S. cryptosystem would first encrypt the data stream and forward the cipher stream to the Russian cryptographic equipment. Presumably, they would buffer, reclock, and gate the cipher stream so as to insure that only the overt channel is available. This is actually a workable scheme—logically. The problem remains that if the host reveals his key, or claims that it has been revealed, the monitor would be unable to persuade an arbiter that a message is authentic since he could know the other parties' key and hence might have the capability to utter a forgery and consequently cannot prove that he did not. A solution, and indeed perhaps the only logically complete one, is to require at least three participants; the host, the monitor, and the arbiter(s). Each supplies a two-key authentication channel, with the secret encryption key stored securely downhole and the decryption key shared with all parties. While it true that each party can perform any operations that his, supposedly secret, downhole equipment can, this does not make it possible for him to utter an acceptable forgery since the other cryptosystems are inscrutable to him. Furthermore, any party by publicizing the secret information he was supposed to protect can only make it possible for the other parties to duplicate the actions of two out of the three or more encryption systems. This concatenated encryption system renders it impossible for the host to disavow incriminating messages by unilaterally compromising his key. From the monitor's standpoint, even if the host and the arbiter(s) collude to deceive him, he will still be able to establish, to his satisfaction, the authenticity of messages. In the improbable event that all of the other parties gang up on the monitor, the monitor will still know whether a message is authentic or not but will be unable to persuade impartial (and uninvolved) observers that he is telling the truth. In other words, the worst that can happen, from the monitor's standpoint, for this fourth-generation system is that he can with low probability find himself in the same situation that he was faced with with certainty in the third-generation system. It should be noted that the three participants need not use the same cryptoalgorithm, the same key sizes, etc. All that is required is that each provide a two-key authentication channel and share their decode key with all other participants. The properties that the resulting system have are the following:

1. No party nor cabal of parties can forge messages that would be accepted as authentic by others.
2. No part of the message is concealed, in particular from the host.
3. The host, the monitor, the arbiters, and other third parties are all able to independently verify the authenticity of messages and to logically prove their authenticity to others.
4. No unilateral action by any of the participants can lessen the confidence of any other party as to the authenticity of messages.
5. No benefit or advantage accrues to the supplier of the hardware.

6 CONCLUDING REMARKS

No further subtleties to the technical problem of how to make the data acquired in various treaty verification systems be trustworthy have been found in the last several years so that there is reason to believe that the problem has finally been solved. In the application addressed in this chapter there is no information to be gained from covertly communicating the identity of the seismic site from which a particular piece of data came, since that is known *a priori* to all participants. Therefore, the order in which the various parties have their encryption operations concatenated does not matter. There are treaty verification systems in which these conditions do not hold, that is, in which the identity of the site from which the data came must be concealed from one or more of the participants, and in which, consequently, the order of the concatenation is vital to the system functioning. It is the author's intention to investigate concatenated cryptosystems, that is, either authentication channels or secrecy channels or mixes of the two, as a generic means by which mutually distrustful and deceitful parties can realize a data communications system they both can trust under a wide variety of circumstances. However, the classic problem of message authentication without secrecy in which disputes can always be logically arbitrated, as typified by a system to verify compliance with a comprehensive nuclear weapons test-ban treaty, appears to have been fully solved by concatenated authentication channels as described here.

REFERENCES

1. E. R. Berlekamp, ***Algebraic Coding Theory.*** New York: McGraw-Hill, 1968.
2. D. E. R. Denning, ***Cryptography and Data Security.*** Reading, MA: Addison-Wesley, 1982.
3. W. Diffie and M. E. Hellman, "New directions in cryptography,'* ***IEEE Trans. Informat. Theory,*** vol. IT-22, no. 6, pp. 644-654, Nov. 1976.
4. R. A. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," ***Commun. Ass. Comput. Mach.,*** vol. 21, no. 2, pp. 120-126, 1978.
5. G. J. Simmons, "Symmetric and asymmetric encryption," ***Computing Surveys,*** vol. 11, no. 4, pp. 305-330, Dec. 1979.
6. ——— , "Secure communications in the presence of pervasive deceit," ***Proc. IEEE Computer Society 1980 Symp. on Security and Privacy*** (G. **Davida,** ed.) (Oakland, CA), Apr. 14-16, 1980, pp. 84-92; 1980.
7. ——— , "Message authentication without secrecy," ***Secure Communications and Asymmetric Cryptosystems, G.*** J. Simmons, Ed. Boulder, CO: Westview Press, 1982, pp. 105-139.
8. ——— , "Verification of treaty compliance-Revisited," ***Proc. IEEE Computer Society 1983 Symp. on Security and Privacy*** (R. Blakley and D. Denning, eds.) (Oakland, CA), Apr. 25-27, 1983, pp. 61-66, 1983.
9. ——— , "Cryptology," ***Encyclopaedia Britannica 16th Edition.*** Chicago, IL: **Ency**clopaedia Britannica, Inc., 1986, pp. 913-924B.
10. G. J. Simmons, R. E. D. Stewart, and F? A. Stokes, "Digital **data** authenticator," Patent Application SD2654, **S42640,** June 30, 1972.