A CYPHERPUNK'S MANIFESTO

Eric Hughes

March 9, 1993

Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world.

If two parties have some sort of dealings, then each has a memory of their interaction. Each party can speak about their own memory of this; how could anyone prevent it? One could pass laws against it, but the freedom of speech, even more than privacy, is fundamental to an open society; we seek not to restrict any speech at all. If many parties speak together in the same forum, each can speak to all the others and aggregate together knowledge about individuals and other parties. The power of electronic communications has enabled such group speech, and it will not go away merely because we might want it to.

Since we desire privacy, we must ensure that each party to a transaction have knowledge only of that which is directly necessary for that transaction. Since any information can be spoken of, we must ensure that we reveal as little as possible. In most cases personal identity is not salient. When I purchase a magazine at a store and hand cash to the clerk, there is no need to know who I am. When I ask my electronic mail provider to send and receive messages, my provider need not know to whom I am speaking or what I am saying or what others are saying to me; my provider only need know how to get the message there and how much I owe them in fees. When my identity is revealed by the underlying mechanism of the transaction, I have no privacy. I cannot here selectively reveal myself; I must _always_ reveal myself.

Therefore, privacy in an open society requires anonymous transaction systems. Until now, cash has been the primary such system. An anonymous transaction system is not a secret transaction system. An anonymous system empowers individuals to reveal their identity when desired and only when desired; this is the essence of privacy.

Privacy in an open society also requires cryptography. If I say something, I want it heard only by those for whom I intend it. If the content of my speech is available to the world, I have no privacy. To encrypt is to indicate the desire for privacy, and to encrypt with weak cryptography is to indicate not too much desire for privacy. Furthermore, to reveal one's identity with assurance when the default is anonymity requires the cryptographic signature.

We cannot expect governments, corporations, or other large, faceless organizations to grant us privacy out of their beneficence. It is to their advantage to speak of us, and we should expect that they will speak. To try to prevent their speech is to fight against the realities of information. Information does not just want to be free, it longs to be free. Information expands to fill the available storage space. Information is Rumor's younger, stronger cousin; Information is fleeter of foot, has more eyes, knows more, and understands less than Rumor.

We must defend our own privacy if we expect to have any. We must come together and create systems which allow anonymous transactions to take place. People have been defending their own privacy for centuries with whispers, darkness, envelopes, closed doors, secret handshakes, and couriers. The technologies of the past did not allow for strong privacy, but electronic technologies do.

We the Cypherpunks are dedicated to building anonymous systems. We are defending our privacy with cryptography, with anonymous mail forwarding

systems, with digital signatures, and with electronic money.

Cypherpunks write code. We know that someone has to write software to defend privacy, and since we can't get privacy unless we all do, we're going to write it. We publish our code so that our fellow Cypherpunks may practice and play with it. Our code is free for all to use, worldwide. We don't much care if you don't approve of the software we write. We know that software can't be destroyed and that a widely dispersed system can't be shut down.

Cypherpunks deplore regulations on cryptography, for encryption is fundamentally a private act. The act of encryption, in fact, removes information from the public realm. Even laws against cryptography reach only so far as a nation's border and the arm of its violence. Cryptography will ineluctably spread over the whole globe, and with it the anonymous transactions systems that it makes possible.

For privacy to be widespread it must be part of a social contract. People must come and together deploy these systems for the common good. Privacy only extends so far as the cooperation of one's fellows in society. We the Cypherpunks seek your questions and your concerns and hope we may engage you so that we do not deceive ourselves. We will not, however, be moved out of our course because some may disagree with our goals.

The Cypherpunks are actively engaged in making the networks safer for privacy. Let us proceed together apace.

Onward.

Crypto Glossary

Timothy C. May and Eric Hughes

November 22, 1992

From: tcmay@netcom.com (Timothy C. May)
Subject: Crypto Glossary
Date: Sun, 22 Nov 92 11:50:55 PST

Here's the glossary of crypto terms we passed out in printed form at the first Cypherpunks meeting in September 1992. Some compromises had to be made in going from the printed form to the ASCII of this transmission, so I hope you'll bear with me.

I'm sending it to the entire list because nearly everyone who hears about it says "Is it online?" and wants a copy. If you don't want it, discard it.

I'm not going to be maintaining the "Cypherpunks FAQ," so don't send me corrections or additions.

Enjoy

Tim May

Major Branches of Cryptology (as we see it)

(these sections will introduce the terms in context, though complete definitions will not be given)

Encryption

privacy of messages
using ciphers and codes to protect the secrecy of messages
DES is the most common symmetric cipher (same key for encryption and decryption)
RSA is the most common asymmetric cipher (different keys for encryption and decryption)

Signatures and Authentication

proving who you are
proving you signed a document (and not someone else)

Untraceable Mail

untraceable sending and receiving of mail and messages
focus: defeating eavesdroppers and traffic analysis
DC protocol (dining cryptographers)

Cryptographic Voting

focus: ballot box anonymity
credentials for voting
issues of double voting, security, robustness, efficiency

Digital Cash

focus: privacy in transactions, purchases
unlinkable credentials
blinded notes
"digital coins" may not be possible

Crypto Anarchy

using the above to evade government, to bypass tax collection, etc.
a technological solution to the problem of too much government

Glossary

agoric systems
: open, free market systems in which voluntary transactions are central.

Alice and Bob
: cryptographic protocols are often made clearer by considering parties A and B, or Alice and Bob, performing some protocol. Eve the eavesdropper, Paul the prover, and Vic the verifier are other common stand-in names.

ANDOS
: all or nothing disclosure of secrets.

anonymous credential
: a credential which asserts some right or privilege or fact without revealing the identity of the holder. This is unlike CA driver's licenses.

asymmetric cipher
: same as public key cryptosystem.

authentication
: the process of verifying an identity or credential, to ensure you are who you said you were.

biometric security
: a type of authentication using fingerprints, retinal scans, palm prints, or other physical/biological signatures of an individual.

bit commitment
: e.g., tossing a coin and then committing to the value without being able to change the outcome. The blob is a cryptographic primitive for this.

blinding, blinded signatures
: A signature that the signer does not remember having made. A blind signature is always a cooperative protocol and the receiver of the signature provides the signer with the blinding information.

blob
: the crypto equivalent of a locked box. A cryptographic primitive for bit commitment, with the properties that a blobs can represent a 0 or a 1, that others cannot tell be looking whether itUs a 0 or a 1, that the creator of the blob can "open" the blob to reveal the contents, and that no blob can be both a 1 and a 0. An example of this is a flipped coin covered by a hand.

channel
: the path over which messages are transmitted. Channels may be secure or insecure, and may have eavesdroppers (or enemies, or disrupters, etc.) who alter messages, insert and delete messages, etc. Cryptography is the means by which communications over insecure channels are protected.

chosen plaintext attack
: an attack where the cryptanalyst gets to choose the plaintext to be enciphered, e.g., when possession of an enciphering machine or algorithm is in the possession of the cryptanalyst.

cipher
: a secret form of writing, using substitution or transposition of characters or symbols.

ciphertext
: the plaintext after it has been encrypted.

code
: a restricted cryptosystem where words or letters of a message are replaced by other words chosen from a codebook. Not part of modern cryptology, but still useful.

coin flipping

an important crypto primitive, or protocol, in which the equivalent of flipping a fair coin is possible. Implemented with blobs.

collusion
: wherein several participants cooperate to deduce the identity of a sender or receiver, or to break a cipher. Most cryptosystems are sensitive to some forms of collusion. Much of the work on implementing DC Nets, for example, involves ensuring that colluders cannot isolate message senders and thereby trace origins and destinations of mail.

computationally secure
: where a cipher cannot be broken with available computer resources, but in theory can be broken with enough computer resources. Contrast with unconditionally secure.

countermeasure
: something you do to thwart an attacker.

credential
: facts or assertions about some entity. For example, credit ratings, passports, reputations, tax status, insurance records, etc. Under the current system, these credentials are increasingly being cross-linked. Blind signatures may be used to create anonymous credentials.

credential clearinghouse
: banks, credit agencies, insurance companies, police departments, etc., that correlate records and decide the status of records.

cryptanalysis
: methods for attacking and breaking ciphers and related cryptographic systems. Ciphers may be broken, traffic may be analyzed, and passwords may be cracked. Computers are of course essential.

crypto anarchy
: the economic and political system after the deployment of encryption, untraceable e-mail, digital pseudonyms, cryptographic voting, and digital cash. A pun on "crypto," meaning "hipen," and as when Gore Vidal called William F. Buckley a "crypto fascist."

cryptography
: another name for cryptology.

cryptology
: the science and study of writing, sending, receiving, and deciphering secret messages. Includes authentication, digital signatures, the hiding of messages (steganography), cryptanalysis, and several other fields.

cyberspace
: the electronic domain, the Nets, and computer-generated spaces. Some say it is the "consensual reality" described in "Neuromancer." Others say it is the phone system. Others have work to do.

DC protocol, or DC-Net
: the dining cryptographers protocol. DC-Nets use multiple participants communicating with the DC protocol.

DES
: the Data Encryption Standard, proposed in 1977 by the National Bureau of Standards (now NIST), with assistance from the National Security Agency. Based on the "Lucifer" cipher developed by Horst Feistel at IBM, DES is a secret key cryptosystem that cycles 64-bit blocks of data through multiple permutations with a 56-bit key controlling the routing. "Diffusion" and "confusion" are combined to form a cipher that has not yet been cryptanalyzed (see "DES, Security of"). DES is in use for interbank transfers, as a cipher inside of several RSA-based systems, and is available for PCs.

DES, Security of
: many have speculated that the NSA placed a trapdoor (or back door) in DES to allow it to read DES-encrypted messages. This has

not been proved. It is known that the original Lucifer algorithm used a 128-bit key and that this key length was shortened to 64 bits (56 bits plus 8 parity bits), thus making exhaustive search much easier (so far as is known, brute-force search has not been done, though it should be feasible today). Shamir and Bihan have used a technique called "differential cryptanalysis" to reduce the exhaustive search needed for chosen plaintext attacks (but with no import for ordinary DES).

differential cryptanalysis the Shamir-Biham
technique for cryptanalyzing DES. With a chosen plaintext attack, they've reduced the number of DES keys that must be tried from about 2^56 to about 2^47 or less. Note, however, that rarely can an attacker mount a chosen plaintext attack on DES systems.

digital cash, digital money
Protocols for transferring value, monetary or otherwise, electronically. Digital cash usually refers to systems that are anonymous. Digital money systems can be used to implement any quantity that is conserved, such as points, mass, dollars, etc. There are many variations of digital money systems, ranging from VISA numbers to blinded signed digital coins. A topic too large for a single glossary entry.

digital pseudonym
basically, a "crypto identity." A way for individuals to set up accounts with various organizations without revealing more information than they wish. Users may have several digital pseudonyms, some used only once, some used over the course of many years. Ideally, the pseudonyms can be linked only at the will of the holder. In the simplest form, a public key can serve as a digital pseudonym and need not be linked to a physical identity.

digital signature
Analogous to a written signature on a document. A modification to a message that only the signer can make but that everyone can recognize. Can be used legally to contract at a distance.

digital timestamping
one function of a digital notary public, in which some message (a song, screenplay, lab notebook, contract, etc.) is stamped with a time that cannot (easily) be forged.

dining cryptographers protocol (aka DC protocol, DC nets)
the untraceable message sending system invented by David Chaum. Named after the "dining philosophers" problem in computer science, participants form circuits and pass messages in such a way that the origin cannot be deduced, barring collusion. At the simplest level, two participants share a key between them. One of them sends some actual message by bitwise exclusive-ORing the message with the key, while the other one just sends the key itself. The actual message from this pair of participants is obtained by XORing the two outputs. However, since nobody but the pair knows the original key, the actual message cannot be traced to either one of the participants.

discrete logarithm problem
given integers a, n, and x, find some integer m such that a^m mod n = x, if m exists. Modular exponentiation, the a^m mod n part, is straightforward (and special purpose chips are available), but the inverse problem is believed to be very hard, in general. Thus it is conjectured that modular exponentiation is a one-way function.

DSS, Digital Signature Standard
the latest NIST (National Institute of Standards and Technology, successor to NBS) standard for digital signatures. Based on the El Gamal cipher, some consider it weak and

poor substitute for RSA-based signature schemes.

eavesdropping, or passive wiretapping
: intercepting messages without detection. Radio waves may be intercepted, phone lines may be tapped, and computers may have RF emissions detected. Even fiber optic lines can be tapped.

factoring
: Some large numbers are difficult to factor. It is conjectured that there are no feasible-- i.e."easy," less than exponential in size of number-- factoring methods. It is also an open problem whether RSA may be broken more easily than by factoring the modulus (e.g., the public key might reveal information which simplifies the problem). Interestingly, though factoring is believed to be "hard", it is not known to be in the class of NP-hard problems. Professor Janek invented a factoring device, but he is believed to be fictional.

information-theoretic security "unbreakable"
: security, in which no amount of cryptanalysis can break a cipher or system. One time pads are an example (providing the pads are not lost nor stolen nor used more than once, of course). Same as unconditionally secure.

key
: a piece of information needed to encipher or decipher a message. Keys may be stolen, bought, lost, etc., just as with physical keys.

key exchange, or key distribution
: the process of sharing a key with some other party, in the case of symmetric ciphers, or of distributing a public key in an asymmetric cipher. A major issue is that the keys be exchanged reliably and without compromise. Diffie and Hellman devised one such scheme, based on the discrete logarithm problem.

known-plaintext attack
: a cryptanalysis of a cipher where plaintext-ciphertext pairs are known. This attack searches for an unknown key. Contrast with the chosen plaintext attack, where the cryptanalyst can also choose the plaintext to be enciphered.

mail, untraceable
: a system for sending and receiving mail without traceability or observability. Receiving mail anonymously can be done with broadcast of the mail in encrypted form. Only the intended recipient (whose identity, or true name, may be unknown to the sender) may able to decipher the message. Sending mail anonymously apparently requires mixes or use of the dining cryptographers (DC) protocol.

minimum disclosure proofs
: another name for zero knowledge proofs, favored by Chaum.

mixes
: David Chaum's term for a box which performs the function of mixing, or decorrelating, incoming and outgoing electronic mail messages. The box also strips off the outer envelope (i.e., decrypts with its private key) and remails the message to the apress on the inner envelope. Tamper-resistant modules may be used to prevent cheating and forced disclosure of the mapping between incoming and outgoing mail. A sequence of many remailings effectively makes tracing sending and receiving impossible. Contrast this with the software version, the DC protocol.

modular exponentiation
: raising an integer to the power of another integer, modulo some integer. For integers a, n, and m, a^m mod n. For example, 5^3 mod 100 = 25. Modular exponentiation can be done fairly quickly with a sequence of bit shifts and aps, and special purpose chips

have been designed. See also discrete logarithm.

National Security Agency (NSA)
: the largest intelligence agency, responsible for making and breaking ciphers, for intercepting communications, and for ensuring the security of U.S. computers. Headquartered in Fort Meade, Maryland, with many listening posts around the world. The NSA funds cryptographic research and advises other agencies about cryptographic matters. The NSA once obviously had the world's leading cryptologists, but this may no longer be the case.

negative credential
: a credential that you possess that you don't want any one else to know, for example, a bankruptcy filing. A formal version of a negative reputation.

NP-complete
: a large class of difficult problems. "NP" stands for nondeterministic polynomial time, a class of problems thought in general not to have feasible algorithms for their solution. A problem is "complete" if any other NP problem may be reduced to that problem. Many important combinatorial and algebraic problems are NP-complete: the traveling salesman problem, the Hamiltonian cycle problem, the word problem, and on and on.

oblivious transfer
: a cryptographic primitive that involves the probabilistic transmission of bits. The sender does not know if the bits were received.

one-time pad
: a string of randomly-selected bits or symbols which is combined with a plaintext message to produce the ciphertext. This combination may be shifting letters some amount, bitwise exclusive-ORed, etc.). The recipient, who also has a copy of the one time pad, can easily recover the plaintext. Provided the pad is only used once and then destroyed, and is not available to an eavesdropper, the system is perfectly secure, i.e., it is information-theoretically secure. Key distribution (the pad) is obviously a practical concern, but consider CD-ROM's.

one-way function
: a function which is easy to compute in one direction but hard to find any inverse for, e.g. modular exponentiation, where the inverse problem is known as the discrete logarithm problem. Compare the special case of trap door one-way functions. An example of a one-way operation is multiplication: it is easy to multiply two prime numbers of 100 digits to produce a 200-digit number, but hard to factor that 200-digit number.

P ?=? NP
: Certainly the most important unsolved problem in complexity theory. If P = NP, then cryptography as we know it today does not exist. If P = NP, all NP problems are "easy."

paping
: sending extra messages to confuse eavesdroppers and to defeat traffic analysis. Also aping random bits to a message to be enciphered.

plaintext
: also called cleartext, the text that is to be enciphered.

Pretty Good Privacy (PGP)
: Phillip Zimmerman's implementation of RSA, recently upgraded to version 2.0, with more robust components and several new features. RSA Data Security has threatened PZ so he no longer works on it. Version 2.0 was written by a consortium of non-U.S. hackers.

prime numbers

integers with no factors other than themselves and 1. The number of primes is unbounded. About 1% of the 100 decimal digit numbers are prime. Since there are about 10^70 particles in the universe, there are about 10^23 100 digit primes for each and every particle in the universe!

probabilistic encryption
a scheme by Goldwasser, Micali, and Blum that allows multiple ciphertexts for the same plaintext, i.e., any given plaintext may have many ciphertexts if the ciphering is repeated. This protects against certain types of known ciphertext attacks on RSA.

proofs of identity
proving who you are, either your true name, or your digital identity. Generally, possession of the right key is sufficient proof (guard your key!). Some work has been done on "is-a-person" credentialling agencies, using the so-called Fiat-Shamir protocol...think of this as a way to issue unforgeable digital passports. Physical proof of identity may be done with biometric security methods. Zero knowledge proofs of identity reveal nothing beyond the fact that the identity is as claimed. This has obvious uses for computer access, passwords, etc.

protocol
a formal procedure for solving some problem. Modern cryptology is mostly about the study of protocols for many problems, such as coin-flipping, bit commitment (blobs), zero knowledge proofs, dining cryptographers, and so on.

public key
the key distributed publicly to potential message-senders. It may be published in a phonebook-like directory or otherwise sent. A major concern is the validity of this public key to guard against spoofing or impersonation.

public key cryptosystem
the modern breakthrough in cryptology, designed by Diffie and Hellman, with contributions from several others. Uses trap door one-way functions so that encryption may be done by anyone with access to the "public key" but decryption may be done only by the holder of the "private key." Encompasses public key encryption, digital signatures, digital cash, and many other protocols and applications.

public key encryption
the use of modern cryptologic methods to provided message security and authentication. The RSA algorithm is the most widely used form of public key encryption, although other systems exist. A public key may be freely published, e.g., in phonebook-like directories, while the corresponding private key is closely guarded.

public key patents
M.I.T. and Stanford, due to the work of Rivest, Shamir, Adleman, Diffie, Hellman, and Merkle, formed Public Key Partners to license the various public key, digital signature, and RSA patents. These patents, granted in the early 1980s, expire in the between 1998 and 2002. PKP has licensed RSA Data Security Inc., of Redwood City, CA, which handles the sales, etc.

quantum cryptography
a system based on quantum-mechanical principles. Eavesdroppers alter the quantum state of the system and so are detected. Developed by Brassard and Bennett, only small laboratory demonstrations have been made.

reputations
the trail of positive and negative associations and judgments that some entity accrues. Credit ratings, academic credentials, and trustworthiness are all examples. A digital pseudonym will accrue these reputation credentials based on actions, opinions of

others, etc. In crypto anarchy, reputations and agoric systems will be of paramount importance. There are many fascinating issues of how reputation-based systems work, how credentials can be bought and sold, and so forth.

RSA

the main public key encryption algorithm, developed by Ron Rivest, Adi Shamir, and Kenneth Adleman. It exploits the difficulty of factoring large numbers to create a private key and public key. First invented in 1978, it remains the core of modern public key systems. It is usually much slower than DES, but special-purpose modular exponentiation chips will likely speed it up. A popular scheme for speed is to use RSA to transmit session keys and then a high-speed cipher like DES for the actual message text.

Description

Let p and q be large primes, typically with more than 100 digits. Let n = pq and find some e such that e is relatively prime to (p - 1)(q - 1). The set of numbers p, q, and e is the private key for RSA. The set of numbers n and e forms the public key (recall that knowing n is not sufficient to easily find p and q...the factoring problem). A message M is encrypted by computing M^e mod n. The owner of the private key can decrypt the encrypted message by exploiting number theory results, as follows. An integer d is computed such that ed =1 (mod (p - 1)(q - 1)). Euler proved a theorem that M^(ed) = M mod n and so M^(ed) mod n = M. This means that in some sense the integers e and d are "inverses" of each other. [If this is unclear, please see one of the many texts and articles on public key encryption.]

secret key cryptosystem

A system which uses the same key to encrypt and decrypt traffic at each end of a communication link. Also called a symmetric or one-key system. Contrast with public key cryptosystem.

smart cards

a computer chip embeped in credit card. They can hold cash, credentials, cryptographic keys, etc. Usually these are built with some degree of tamper-resistance. Smart cards may perform part of a crypto transaction, or all of it. Performing part of it may mean checking the computations of a more powerful computer, e.g., one in an ATM.

spoofing, or masquerading

posing as another user. Used for stealing passwords, modifying files, and stealing cash. Digital signatures and other authentication methods are useful to prevent this. Public keys must be validated and protected to ensure that others don't substitute their own public keys which users may then unwittingly use.

steganography

a part of cryptology dealing with hiding messages and obscuring who is sending and receiving messages. Message traffic is often paped to reduce the signals that would otherwise come from a supen beginning of messages.

symmetric cipher

same as private key cryptosystem.

tamper-responding modules, tamper-resistant modules (TRMs)

sealed boxes or modules which are hard to open, requiring extensive probing and usually leaving ample evidence that the tampering has occurred. Various protective techniques are used, such as special metal or oxide layers on chips, armored coatings, embeped optical fibers, and other measures to thwart analysis. Popularly called "tamper-

proof boxes." Uses include: smart cards, nuclear weapon initiators, cryptographic key holders, ATMs, etc.

tampering, or active wiretapping
: interfering with messages and possibly modifying them. This may compromise data security, help to break ciphers, etc. See also spoofing.

token
: some representation, such as ID cards, subway tokens, money, etc., that indicates possession of some property or value.

traffic analysis
: determining who is sending or receiving messages by analyzing packets, frequency of packets, etc. A part of steganography. Usually handled with traffic paping.

transmission rules
: the protocols for determining who can send messages in a DC protocol, and when. These rules are needed to prevent collision and deliberate jamming of the channels.

trap messages
: dummy messages in DC Nets which are used to catch jammers and disrupters. The messages contain no private information and are published in a blob beforehand so that the trap message can later be opened to reveal the disrupter. (There are many strategies to explore here.)

trap-door
: In cryptography, a piece of secret information that allows the holder of a private key to invert a normally hard to invert function.

trap-door one way functions
: functions which are easy to compute in both the forward and reverse direction but for which the disclosure of an algorithm to compute the function in the forward direction does not provide information on how to compute the function in the reverse direction. More simply put, trap-door one way functions are one way for all but the holder of the secret information. The RSA algorithm is the best-known example of such a function.

unconditional security
: same as information-theoretic security, that is, unbreakable except by loss or theft of the key.

unconditionally secure
: where no amount of intercepted ciphertext is enough to allow the cipher to be broken, as with the use of a one-time pad cipher. Contrast with computationally secure.

voting, cryptographic
: Various schemes have been devised for anonymous, untraceable voting. Voting schemes should have several properties: privacy of the vote, security of the vote (no multiple votes), robustness against disruption by jammers or disrupters, verifiability (voter has confidence in the results), and efficiency.

zero knowledge proofs
: proofs in which no knowledge of the actual proof is conveyed. Peggy the Prover demonstrates to Sid the Skeptic that she is indeed in possession of some piece of knowledge without actually revealing any of that knowledge. This is useful for access to computers, because eavesdroppers or dishonest sysops cannot steal the knowledge given. Also called minimum disclosure proofs. Useful for proving possession of some property, or credential, such as age or voting status, without revealing personal information.