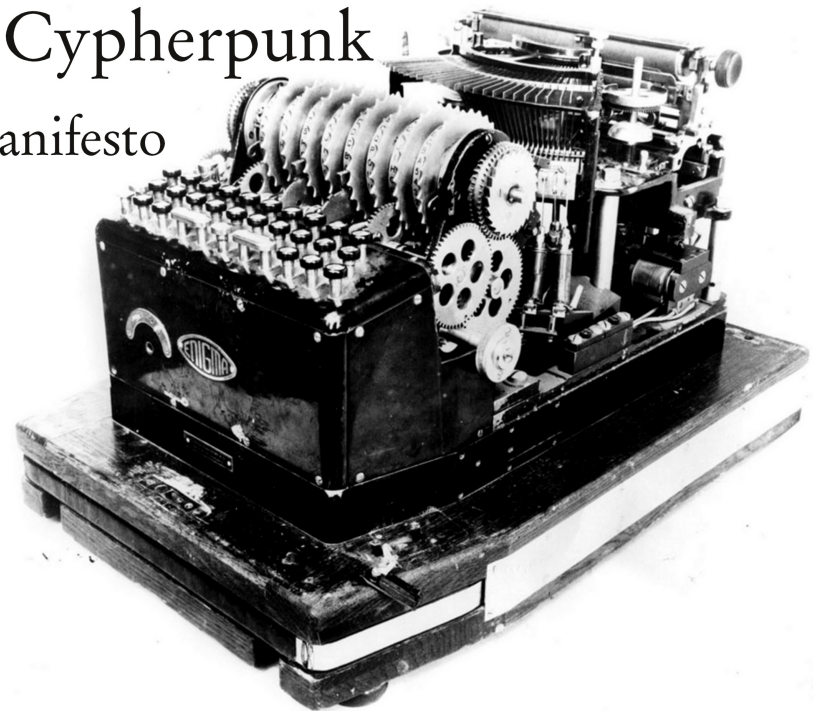


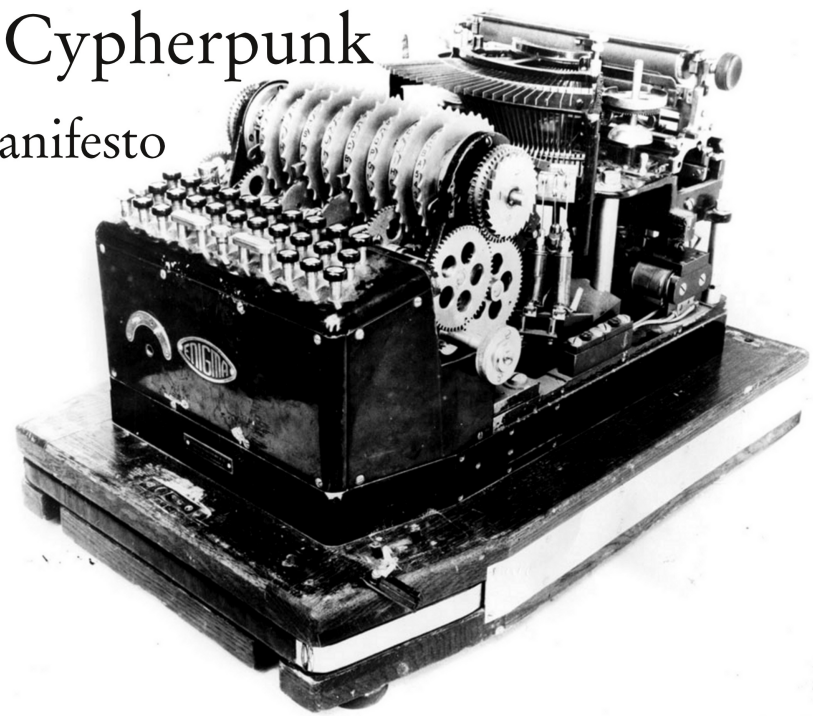
hQEMA0senuCtDLyMAQf/YSpRE8ZF4w5rJw2qsNjrWd5nBesrD1+e  
NzuQVTBucMgiLQUHiEs6sezsRmQy5hJkiUfVYcHeJSM3xYzsJVrz  
mPpZkFEyMuuLlyFNm9NUHZI5yj//uEVkMYD/vPro/uvSzZHDqnAA  
GYbqGCSEkjJ3uwT2bpFEHcbN4SSauXvs6g2AwB+4Mbac28Rp3awq  
W6Vqr+rchvdfEhb306iim5DoH6vugNxjmBgEmeJ3AodbHOdocWXw  
MR0dKXpL4zdXYSLajaE941IBwGxQq0eYOEo4vtSNyoCGK1eT20Qj  
vewabGP3tclb5RxdFtLe8nlvIYd8VSmbLRboslnZ7IaMaG19MoUB  
DANaNEMLJJC SugEIAIdiZNDlNLkMWgkB0mb7A+mgvdAETTC1rs2z  
VAnAh9P5z0x0mu/r1tcQuSJ4KESvhs1qS6crWGjIzmTGf76qZ5AR  
B9rC3Db1goEbbaeTKOWxekLLymZQY2aj9fglEPkgoXFNRnOIJwx  
PinTc36CLG8XxODO8weFJYEKPs88FiHKyz7gFNf0Gx37m1FDH9r+  
uv/VJKKw8M6w=**CY4H3R4UNK5+WR173+C0D3**=uGFbYABzBARr2TwA  
E2iuAjQXGggSQ90UhNuv/pHvWy9/yUiEgKZngAnk8VG8jYJeH6yS  
UPf3VkrhC9tNeOd66ZmpLLNHjiU2T8TH0TCrb0NOE/x1VxUuVUW6

hQEMA0senuCtDLyMAQf/YSpRE8ZF4w5rJw2qsNjrWd5nBesrD1+e  
NzuQVTBucMgiLQUHiEs6sezsRmQy5hJkiUfVYcHeJSM3xYzsJVrz  
mPpZkFEyMuuLlyFNm9NUHZI5yj//uEVkMYD/vPro/uvSzZHDqnAA  
GYbqGCSEkjJ3uwT2bpFEHcbN4SSauXvs6g2AwB+4Mbac28Rp3awq  
W6Vqr+rchvdfEhb306iim5DoH6vugNxjmBgEmeJ3AodbHOdocWXw  
MR0dKXpL4zdXYSLajaE941IBwGxQq0eYOEo4vtSNyoCGK1eT20Qj  
vewabGP3tclb5RxdFtLe8nlvIYd8VSmbLRboslnZ7IaMaG19MoUB  
DANaNEMLJJC SugEIAIdiZNDlNLkMWgkB0mb7A+mgvdAETTC1rs2z  
VAnAh9P5z0x0mu/r1tcQuSJ4KESvhs1qS6crWGjIzmTGf76qZ5AR  
B9rC3Db1goEbbaeTKOWxekLLymZQY2aj9fglEPkgoXFNRnOIJwx  
PinTc36CLG8XxODO8weFJYEKPs88FiHKyz7gFNf0Gx37m1FDH9r+  
uv/VJKKw8M6w=**CY4H3R4UNK5+WR173+C0D3**=uGFbYABzBARr2TwA  
E2iuAjQXGggSQ90UhNuv/pHvWy9/yUiEgKZngAnk8VG8jYJeH6yS  
UPf3VkrhC9tNeOd66ZmpLLNHjiU2T8TH0TCrb0NOE/x1VxUuVUW6

## A Cypherpunk Manifesto



## A Cypherpunk Manifesto



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.

Eric Hughes <hughes@soda.berkeley.edu >  
9 March 1993

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.

Eric Hughes <hughes@soda.berkeley.edu >  
9 March 1993

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

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

## A Cypherpunk's Manifesto by Eric Hughes

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,

## A Cypherpunk's Manifesto by Eric Hughes

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

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

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,

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,



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

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

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

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.

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 fleet of foot, has more eyes,

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 fleet of foot, has more eyes,