Subject: The Crypto Anarchist Manifesto
Date: Sun, 22 Nov 92 12:11:24 PST

Cypherpunks of the World,

Several of you at the "physical Cypherpunks" gathering yesterday in Silicon Valley requested that more of the material passed out in meetings be available electronically to the entire readership of the Cypherpunks list, spooks, eavesdroppers, and all. <Gulp>

Here's the "Crypto Anarchist Manifesto" I read at the September 1992 founding meeting. It dates back to mid-1988 and was distributed to some like-minded techno-anarchists at the "Crypto '88" conference and then again at the "Hackers Conference" that year. I later gave talks at Hackers on this in 1989 and 1990.

There are a few things I'd change, but for historical reasons I'll just leave it as is. Some of the terms may be unfamiliar to you...I hope the Crypto Glossary I just distributed will help.

(This should explain all those cryptic terms in my .signature!)

--Tim May

.....

The Crypto Anarchist Manifesto

Timothy C. May <tcmay@netcom.com>

A specter is haunting the modern world, the specter of crypto anarchy.

Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner. Two persons may exchange messages, conduct business, and negotiate electronic contracts without ever knowing the True Name, or legal identity, of the other. Interactions over networks will be untraceable, via extensive re-routing of encrypted packets and tamper-proof boxes which implement cryptographic protocols with nearly perfect assurance against any tampering. Reputations will be of central importance, far more important in dealings than even the credit ratings of today. These developments will alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation.

The technology for this revolution--and it surely will be both a social and economic revolution--has existed in theory for the past

decade. The methods are based upon public-key encryption, zero-knowledge interactive proof systems, and various software protocols for interaction, authentication, and verification. The focus has until now been on academic conferences in Europe and the U.S., conferences monitored closely by the National Security Agency. But only recently have computer networks and personal computers attained sufficient speed to make the ideas practically realizable. And the next ten years will bring enough additional speed to make the ideas economically feasible and essentially unstoppable. High-speed networks, ISDN, tamper-proof boxes, smart cards, satellites, Ku-band transmitters, multi-MIPS personal computers, and encryption chips now under development will be some of the enabling technologies.

The State will of course try to slow or halt the spread of this technology, citing national security concerns, use of the technology by drug dealers and tax evaders, and fears of societal disintegration. Many of these concerns will be valid; crypto anarchy will allow national secrets to be trade freely and will allow illicit and stolen materials to be traded. An anonymous computerized market will even make possible abhorrent markets for assassinations and extortion. Various criminal and foreign elements will be active users of CryptoNet. But this will not halt the spread of crypto anarchy.

Just as the technology of printing altered and reduced the power of medieval guilds and the social power structure, so too will cryptologic methods fundamentally alter the nature of corporations and of government interference in economic transactions. Combined with emerging information markets, crypto anarchy will create a liquid market for any and all material which can be put into words and pictures. And just as a seemingly minor invention like barbed wire made possible the fencing-off of vast ranches and farms, thus altering forever the concepts of land and property rights in the frontier West, so too will the seemingly minor discovery out of an arcane branch of mathematics come to be the wire clippers which dismantle the barbed wire around intellectual property.

Arise, you have nothing to lose but your barbed wire fences!

--
.....
Timothy C. May | Crypto Anarchy: encryption, digital money,
tcmay@netcom.com | anonymous networks, digital pseudonyms, zero
408-688-5409 | knowledge, reputations, information markets,
W.A.S.T.E.: Aptos, CA | black markets, collapse of governments.
Higher Power: 2^756839 | PGP Public Key: by arrangement.

Manifest kryptoanarchie

Moderním světem prochází přízrak, přízrak krypto-anarchie.

Výpočetní technika stojí na bodu na zlomu, kdy bude schopna poskytnout jednotlivcům i celým skupinám možnost komunikovat navzájem v naprosté anonymitě.

Budeme vyměňovat zprávy, uzavírat obchody a vyjednávat smlouvy elektronicky, aniž bychom věděli, pravé jméno, nebo právní status druhé strany. Operace napříč sítěmi budou nevystopovatelné prostřednictvím šifrovaných aplikací, které implementují kryptografické protokoly s téměř dokonalými pojistkami proti prolomení.Pověst bude mít zásadní význam. V obchodním styku bude hrát mnohem důležitější roli, než jakou hrají dnes roli hodnocení a reference. Tento vývoj bude od základu měnit povahu vládní regulace, schopnost danit a regulovat ekonomické vztahy, schopnost udržet informace v tajnosti.

Technologie pro tuto revoluci - a jistě to bude revoluce společenská i ekonomická - existuje na úrovni teorie posledních deset let. Metody jsou založeny na šifrování pomocí veřejného klíče, systémech prokazování bez jakékoliv další informace, a různé softwarové protokoly pro interakci, ověřování a potvrzování.

Teprve v poslední době dosahují počítačové sítě a osobní počítače dostatečnou rychlost, aby tyto myšlenky byly prakticky uskutečnitelné. A příští desetiletí přinese další přidanou rychlost, která umožní jejich ekonomickou proveditelnost a v podstatě nezastavitelnost. Vysokorychlostní sítě, ISDN, schránky odolné proti prolomení, čipové karty, satelity, satelitní vysílače , osobní počítače s vysokou operační pamětí a šifrované čipy a ve fázi vývoje jsou další z budoucích klíčových technologií.

Státy se samozřejmě budou snažit zpomalit nebo zastavit šíření této technologie, budou zmiňovat obavy o národní bezpečnost, hrozby využívání technologií drogovými dealery a daňovými podvodníky, a budou hrozit obavami ze společenské dezintegrace. Mnohé z těchto obav budou na místě. Kryptoanarchie umožní volné nakládání s národním tajemstvím a umožní, aby se obchodovalo s ilegálními a ukradenými materiály. Anonymní elektronický trh bude dokonce umožňovat odporné trhy s vraždami a vydíráním. Různé kriminální a cizorodé živly budou aktivními uživateli krypto-sítě. To ale šíření kryptoanarchie nezastaví.

Stejně jako technologie tisku změnila a zmírnila sílu středověkých cechů a struktury společenské moci, tak i kryptologické metody zásadně změní povahu korporací a vládních zásahů do ekonomických transakcí. V kombinaci s novými informačními trhy, bude kryptoanarchie tvořit tekutý trh pro veškerý materiál, který lze vyjádřit slovy nebo obrazy. A stejně jako zdánlivě nevýznamný vynález ostnatého drátu umožnil oplocení rozlehlých farem a zemědělských podniků, a tím navždy změnil pojetí pozemku a vlastnických práv na západě, tak i zdánlivě malý objev z tajemného odvětví matematiky přišel s kleštěmi, které odstraní ostnatý drát kolem duševního vlastnictví.

Povstaňte, nemáte co ztratit, leda své ostnaté dráty!

Kryptoanarchistické manifesto

Moderným svetom sa začala šíriť nová vlna, vlna kryptoanarchie.

Technológia dosiahne úroveň, ktorá dokáže zaručiť slobodu a anonymitu úplne každému. Bude možné slobodne komunikovať, obchodovať a uzatvárať dohody bez toho, aby sme navzájom poznali svoju skutočnú identitu. Interakcie cez počítačové siete budú nevystopovateľné, cez prestupné stanice posielajúce zašifrované pakety a krabičky zabezpečené proti manipulácii, ktoré implementujú kryptografické protokoly s takmer dokonalou ochranou proti odpočúvaniu a manipulácii.
Kryptografia nám poskytuje nevystopovateľnosť, vďaka ktorej si budeme vedieť ochrániť súkromie. Naša elektronická reputácia nadobudne omnoho väčšieho významu než protekcia, povery či neobjektívne hodnotenia z minulosti. Takýto vývoj nedokáže zastaviť žiaden politik, vláda ani organizácia a budú sa mu musieť prispôsobiť. Akékoľvek nezmyselné regulácie a príkazy stratia zmysel, vlády stratia schopnosť zdaňovať a vstupovať do ekonomických interakcií tretích strán. Koncept dôvery sa od základov zmení.

Táto revolučná technológia dokáže zmeniť celý ekonomický a spoločenský systém a na jej tvorení sa už pracuje desiatky rokov. Vďaka úžasnému pokroku v rýchlosti počítačov dokážeme realizovať metódy asymetrického šifrovania, zero-knowledge dôkazov, ich verifikácie a množstvo protokolov na interakciu, autentikáciu a verifikáciu na škále omnoho väčšej, než sa kedy podarilo na prísne sledovaných bezpečnostných konferenciách. Ďalšie roky nepochybne prinesú mnoho kľúčových technológií.

Štáty budú prirodzene usilovať o spomalenie a kontrolu takýchto technológií. Argumentmi sa stanú otázky národnej bezpečnosti, zneužitie predajcami drog, daňových optimalizátorov a rozpad spoločnosti. Väčšina z týchto obáv je úplne na mieste. Kryptoanarchia totiž nebude brániť voľnému šíreniu štátnych tajomstiev a obchodu s ilegálnym tovarom. Anonymné počítačové trhy dokonca umožnia vytvorenie obchodu s vraždami a vydieraním. Mnohé zločinecké organizácie a zahraničné agentúry budú aktívnymi používateľmi CryptoNetu. Ale ani toto všetko nezastaví rozšírenie kryptoanarchie.

Podobne ako príchod technológie tlače kedysi zmenil štruktúru vládnej moci, aj kryptografia zásadne ovplyvní povahu korporácií a účinnosť vládnych zásahov do ekonomických transakcií. V kombinácii s informačnými trhmi vznikne voľný trh pre všetko, čo je možné vyjadriť slovami, obrázkami alebo dátami. Kedysi bola konštrukcia ostnatého drôtu zdanlivo banálnym vynálezom, vďaka ktorému bolo možné ohradiť ranče, farmy a navždy ovplyvniť koncept pozemkových a vlastníckych práv na Západe. Tajomné odvetvie matematiky prináša kliešte, ktorými môžeme odstrániť ostnatý drôt, ktorý chráni “duševné vlastníctvo”.

Nemáme sa čoho báť, prísť môžeme len o tie ostnaté drôty.