FROM CROSSBOWS TO CRYPTOGRAPHY: THWARTING THE STATE VIA TECHNOLOGY

CHUCK HAMMILL

$$xy = \{(p-1)(q-1) + 1\}$$

The following is the text of a talk given by Chuck Hammill to the Future of Freedom Conference, in Culver City, California, in November 1987.

You know, technology - and particularly computer technology - has often gotten a bad rap in Libertarian circles. We tend to think of Orwell's *1984*, or Terry Gilliam's *Brazil*, or the proximity detectors keeping East Berlin's slave/citizens on their own side of the border, or the sophisticated bugging devices Nixon used to harass those on his "enemies list". Or, we recognize that for the price of a ticket on the Concorde we can fly at twice the speed of sound, but only if we first walk thru a magnetometer run by a government policeman, and permit him to paw through our belongings if it beeps.

But I think that mind-set is a mistake. Before there were cattle prods, governments tortured their prisoners with clubs and rubber hoses. Before there were lasers for eavesdropping, governments used binoculars and lip-readers. Though government certainly uses technology to oppress, the evil lies not in the tools but in the wielder of the tools.

In fact, technology represents one of the most promising avenues available for re-capturing our freedoms from those who have stolen them. By its very nature, it favors the bright (who can put it to use) over the dull (who cannot). It favors the adaptable (who are quick to see the merit of the new) over the sluggish (who cling to time-tested ways). And what two better words are there to describe government bureaucracy than "dull" and "sluggish"?

EQUALIZERS

One of the clearest, classic triumphs of technology over tyranny I see is the invention of the man-portable crossbow. With it, an untrained peasant could now reliably and lethally engage a target out to fifty meters - even if that target were a mounted, chain-mailed knight. (Unlike the longbow, which admittedly was more powerful, and could get off more shots per unit time, the crossbow required no formal training to utilize. Whereas the longbow required elaborate visual, tactile and kinesthetic coordination to achieve any degree of accuracy, the wielder of a crossbow could simply put the weapon to his shoulder, sight along the arrow itself, and be reasonably assured of hitting his target.)

Moreover, since just about the only mounted knights likely to visit your average peasant would be government soldiers and tax collectors, the utility of the device was plain: With it, the common rabble could defend themselves not only against one another, but against their governmental masters. It was the medieval equivalent of the armor-piercing bullet, and, consequently, kings and priests (the medieval equivalent of a Bureau of Alcohol, Tobacco and Crossbows) threatened death and excommunication, respectively, for its unlawful possession.

Looking at later developments, we see how technology like the firearm - particularly the repeating rifle and the handgun, later followed by the Gatling gun and more advanced machine guns - radically altered the balance of interpersonal and inter-group power. Not without reason was the Colt .45 called "the equalizer". A frail dance-hall hostess with one in her possession was now fully able to protect herself against the brawniest roughneck in any saloon. Advertisements for the period also reflect the merchandising of the repeating cartridge rifle by declaring that "a man on horseback, armed with one of these rifles, simply cannot be captured." And, as long as his captors were relying upon flintlocks or single-shot rifles, the quote is doubtless a true one.

Updating now to the present, the public-key cipher (with a personal computer to run it) represents an equivalent quantum leap - in a defensive weapon. Not only can such a technique be used to protect sensitive data in one's own possession, but it can also permit two strangers to exchange information over an insecure communications channel - a wiretapped phone line, for example, or skywriting, for that matter - without ever having previously met to exchange cipher keys. With a thousand-dollar computer, you can create a cipher that a multi-megabuck CRAY X-MP can't crack in a year. Within a few years, it should be economically feasible to similarly encrypt voice communications; soon after that, full-color digitized video images. Technology will not only have made wiretapping obsolete, it will have totally demolished government's control over information transfer.

A GROUNDBREAKING DEVELOPMENT

I'd like to take just a moment to sketch the mathematics which makes this principle possible. This algorithm is called the RSA algorithm, after Rivest, Shamir, and Adleman who jointly created it. Its security derives from the fact that, if a very large number is the product of two very large primes, then it is extremely difficult to obtain the two prime factors from analysis of their product. "Extremely" in the sense that if primes p and q have 100 digits apiece, then

Scientific Notes No. 9

ISSN 0267-7067 ISBN 1 85637 100 X

An occasional publication of the Libertarian Alliance,
25 Chapter Chambers, Esterbrooke Street, London SW1P 4NN
www.libertarian.co.uk email: admin@libertarian.co.uk

Chuck Hammill is a mathematician and libertarian activist, living in Los Angeles.

Director: Dr Chris R. Tame
Editorial Director: Brian Micklethwait Webmaster: Dr Sean Gabb

FOR LIFE, LIBERTY AND PROPERTY

their 200-digit product cannot in general be factored in less than 100 years by the most powerful computer now in existence.

The "public" part of the key consists of (1) the product pq of the two large primes p and q, and (2) one factor, call it x, of the product xy where xy = {(p-1)(q-1) + 1}. The "private" part of the key consists of the other factor y.

Each block of the text to be encrypted is first turned into an integer - either by using ASCII, or even a simple A = 01, B = 02, C = 03, ... , Z = 26 representation. This integer is then raised to the power x (modulo pq) and the resulting integer is then sent as the encrypted message. The receiver decrypts by taking this integer to the (secret) power y (modulo pq). It can be shown that this process will always yield the original number started with.

What makes this a groundbreaking development, and why it is called "public-key" cryptography, is that I can openly publish the product pq and the number x, while keeping secret the number y - so that anyone can send me an encrypted message, namely x a (mod pq), but only I can recover the original message a, by taking what they send, raising it to the power y and taking the result (mod pq). The risky step (meeting to exchange cipher keys) has been eliminated. So people who may not even trust each other enough to want to meet, may still reliably exchange encrypted messages - each party having selected and disseminated his own pq and his x, while maintaining the secrecy of his own y.

Another benefit of this scheme is the notion of a "digital signature", to enable one to authenticate the source of a given message. Normally, if I want to send you a message, I raise my plaintext a to your x and take the result (mod your pq) and send that.

However, if in my message, I take the plaintext a and raise it to my (secret) power y, take the result (mod my pq), then raise that result to your x (mod your pq) and send this, then even after you have normally "decrypted" the message, it will still look like garbage. However, if you then raise it to my public power x, and take the result (mod my public pq), you will not only recover the original plaintext message, but you will know that no one but I could have sent it to you (since no one else knows my secret y).

THE SOVIET DILEMMA

And these are the very concerns by the way that are today tormenting the Soviet Union about the whole question of personal computers. On the one hand, they recognize that American schoolchildren are right now growing up with computers as commonplace as sliderules used to be - more so, in fact, because there are things computers can do which will interest (and instruct) 3- and 4-year-olds. And it is precisely these students who one generation hence will be going head-to-head against their Soviet counterparts. For the Soviets to hold back might be as suicidal as continuing to teach swordsmanship while your adversaries are learning ballistics. On the other hand, whatever else a personal computer may be, it is also an exquisitely efficient copying machine - a floppy disk will hold upwards of 50,000 words of text, and can be copied in a couple of minutes. If this weren't threatening enough, the computer that performs the copy can also encrypt the data in a fashion that is all but unbreakable. Remember that in Soviet society publicly accessible Xerox machines are unknown. (The relatively few copying machines in existence are controlled more intensively than machine guns are in the United States.)

Now the "conservative" position is that we should not sell these computers to the Soviets, because they could use them in weapons systems. The "liberal" position is that we should sell them, in the interests of mutual trade and cooperation - and anyway, if we don't make the sale, there will certainly be some other nation willing to.

For my part, I'm ready to suggest that the Libertarian position should be to give them to the Soviets for free, and if necessary, make them take them ... and if that doesn't work load up an SR-71 Blackbird and air drop them over Moscow in the middle of the night. Paid for by private subscription, of course, not taxation ... I confess that this is not a position that has gained much support among members of the conventional left-right political spectrum, but, after all, in the words of one of Illuminatus's characters, we are political non-Euclideans: The shortest distance to a particular goal may not look anything like what most people would consider a "straight line". Taking a long enough world-view, it is arguable that breaking the Soviet government monopoly on information transfer could better lead to the enfeeblement and, indeed, to the ultimate dissolution of the Soviet empire than would the production of another dozen missiles aimed at Moscow.

But there's the rub: a "long enough" world view does suggest that the evil, the oppressive, the coercive and the simply stupid will "get what they deserve", but what's not immediately clear is how the rest of us can escape being killed, enslaved, or pauperized in the process.

THE LIBERTARIAN EDGE

When the "liberals" and other collectivists began to attack freedom, they possessed a reasonably stable, healthy, functioning economy, and almost unlimited time to proceed to hamstring and dismantle it. A policy of political gradualism was at least conceivable. But now, we have a patchwork crazy-quilt economy held together by baling wire and spit. The state not only taxes us to "feed the poor" while also inducing farmers to slaughter milk cows and drive up food prices - it then simultaneously turns around and subsidizes research into agricultural chemicals designed to increase yields of milk from the cows left alive. Or witness the fact that a decline in the price of oil is considered as potentially frightening as a comparable increase a few years ago. When the price went up, we were told, the economy risked collapse for for want of energy. The price increase was called the "moral equivalent of war" and the Feds swung into action. For the first time in American history, the speed at which you drive your car to work in the morning became an issue of Federal concern. Now, when the price of oil drops, again we risk problems, this time because American oil companies and Third World basket-case nations who sell oil may not be able to ever pay their debts to our grossly overextended banks. The suggested panacea is that government should now re-raise the oil prices that OPEC has lowered, via a new oil tax. Since the government is seeking to raise oil prices to about the same extent as OPEC did, what can we call this except the "moral equivalent of civil war - the government against its own people?"

And, classically, in international trade, can you imagine any entity in the world except a government going to court claiming that a vendor was selling it goods too cheaply and

demanding not only that that naughty vendor be compelled by the court to raise its prices, but also that it be punished for the act of lowering them in the first place?

So while the statists could afford to take a couple of hundred years to trash our economy and our liberties, we certainly cannot count on having an equivalent period of stability in which to reclaim them. I contend that there exists almost a "black hole" effect in the evolution of nation-states just as in the evolution of stars. Once freedom contracts beyond a certain minimum extent, the state warps the fabric of the political continuum about itself to the degree that subsequent re-emergence of freedom becomes all but impossible. A good illustration of this can be seen in the area of so-called "welfare" payments. When those who sup at the public trough outnumber (and thus outvote) those whose taxes must replenish the trough, then what possible choice has a democracy but to perpetuate and expand the taking from the few for the unearned benefit of the many? Go down to the nearest "welfare" office, find just two people on the dole ... and recognize that between them they form a voting bloc that can forever outvote you on the question of who owns your life - and the fruits of your life's labor.

So essentially those who love liberty need an "edge" of some sort if we're ultimately going to prevail. We obviously can't use the altruists' "other-directedness" of "work, slave, suffer, sacrifice, so that next generation of a billion random strangers can live in a better world." Recognize that, however immoral such an appeal might be, it is nonetheless an extremely powerful one in today's culture. If you can convince people to work energetically for a "cause", caring only enough for their personal welfare so as to remain alive enough and healthy enough to continue working - then you have a truly massive reservoir of energy to draw from. Equally clearly, this is just the sort of appeal which tautologically cannot be utilized for egoistic or libertarian goals. If I were to stand up before you tonight and say something like, "Listen, follow me as I enunciate my noble 'cause', contribute your money to support the 'cause', give up your free time to work for the 'cause', strive selflessly to bring it about, and then (after you and your children are dead) maybe your children's children will actually live under egoism" - you'd all think I'd gone mad. And of course you'd be right. Because the point I'm trying to make is that libertarianism and/or egoism will be spread if, when, and as, individual libertarians and/or egoists find it profitable and/or enjoyable to do so. And probably only then.

While I certainly do not disparage the concept of political action, I don't believe that it is the only, nor even necessarily the most cost-effective path toward increasing freedom in our time. Consider that, for a fraction of the investment in time, money and effort I might expend in trying to convince the state to abolish wiretapping and all forms of censorship - I can teach every libertarian who's interested how to use cryptography to abolish them unilaterally.

EACH PARTY WINS

There is a maxim - a proverb - generally attributed to the Eskimoes, which very likely most Libertarians have already heard. And while you likely would not quarrel with the saying, you might well feel that you've heard it often enough already, and that it has nothing further to teach us, and moreover, that maybe you're even tired of hearing it. I shall therefore repeat it now:

> If you give a man a fish, the saying runs, you feed him for a day. But if you teach a man how to fish, you feed him for a lifetime.

Your exposure to the quote was probably in some sort of a "workfare" vs. "welfare" context; namely, that if you genuinely wish to help someone in need, you should teach him how to earn his sustenance, not simply how to beg for it. And of course this is true, if only because the next time he is hungry, there might not be anybody around willing or even able to give him a fish, whereas with the information on how to fish, he is completely self-sufficient.

But I submit that this exhausts only the first order content of the quote, and if there were nothing further to glean from it, I would have wasted your time by citing it again. After all, it seems to have almost a crypto-altruist slant, as though to imply that we should structure our activities so as to maximize the benefits to such hungry beggars as we may encounter.

But consider. Suppose this Eskimo doesn't know how to fish, but he does know how to hunt walruses. You, on the other hand, have often gone hungry while traveling thru walrus country because you had no idea how to catch the damn things, and they ate most of the fish you could catch. And now suppose the two of you decide to exchange information, bartering fishing knowledge for hunting knowledge. Well, the first thing to observe is that a transaction of this type categorically and unambiguously refutes the Marxist premise that every trade must have a "winner" and a "loser"; the idea that if one person gains, it must necessarily be at the "expense" of another person who loses. Clearly, under this scenario, such is not the case. Each party has gained something he did not have before, and neither has been diminished in any way. When it comes to exchange of information (rather than material objects) life is no longer a zero-sum game. This is an extremely powerful notion. The "law of diminishing returns", the "first and second laws of thermodynamics" - all those "laws" which constrain our possibilities in other contexts- - no longer bind us! Now that's anarchy!

INFORMATION MULTIPLIES EFFICACY

Or consider another possibility. Suppose this hungry Eskimo never learned to fish because the ruler of his nation-state had decreed fishing illegal. Because fish contain dangerous tiny bones, and sometimes sharp spines, he tells us, the state has decreed that their consumption - and even their possession - are too hazardous to the people's health to be permitted . . . even by knowledgeable, willing adults. Perhaps it is because citizens' bodies are thought to be government property, and therefore it is the function of the state to punish those who improperly care for government property. Or perhaps it is because the state generously extends to competent adults the "benefits" it provides to children and to the mentally ill: namely, a full-time, all-pervasive supervisory conservatorship - so that they need not trouble themselves with making choices about behavior thought physically risky or morally "naughty". But, in any case, you stare stupefied, while your Eskimo informant relates how this law is taken so seriously that a friend of his was recently imprisoned for years for the crime of "possession of nine ounces of trout with intent to distribute".

Now you may conclude that a society so grotesquely oppressive as to enforce a law of this type is simply an affront

to the dignity of all human beings. You may go farther and decide to commit some portion of your discretionary, recreational time specifically to the task of thwarting this tyrant's goal. (Your rationale may be "altruistic" in the sense of wanting to liberate the oppressed, or "egoistic" in the sense of proving you can outsmart the oppressor - or very likely some combination of these or perhaps even other motives.)

But, since you have zero desire to become a martyr to your "cause", you're not about to mount a military campaign, or even try to run a boatload of fish through the blockade. However, it is here that technology - and in particular information technology - can multiply your efficacy literally a hundredfold. I say "literally", because for a fraction of the effort (and virtually none of the risk) attendant to smuggling in a hundred fish, you can quite readily produce a hundred Xerox copies of fishing instructions. (If the targeted government, like present-day America, at least permits open discussion of topics whose implementation is restricted, then that should suffice. But, if the government attempts to suppress the flow of information as well, then you will have to take a little more effort and perhaps write your fishing manual on a floppy disk encrypted according to your mythical Eskimo's public-key parameters. But as far as increasing real-world access to fish you have made genuine nonzero headway - which may continue to snowball as others re-disseminate the information you have provided. And you have not had to waste any of your time trying to convert ideological adversaries, or even trying to win over the undecided. Recall Harry Browne's dictum from *How I Found Freedom in an Unfree World* (Macmillan, New York, 1973) that the success of any endeavor is in general inversely proportional to the number of people whose persuasion is necessary to its fulfilment.

If you look at history, you cannot deny that it has been dramatically shaped by men with names like Washington, Lincoln ... Nixon ... Marcos ... Duvalier ... Khadaffi ... and their ilk. But it has also been shaped by people with names like Edison, Curie, Marconi, Tesla and Wozniak. And this latter shaping has been at least as pervasive, and not nearly so bloody.

THE LIBERTECH PROJECT

And that's where I'm trying to take The LiberTech Project. Rather than beseeching the state to please not enslave, plunder or constrain us, I propose a libertarian network spreading the technologies by which we may seize freedom for ourselves.

But here we must be a bit careful. While it is not (at present) illegal to encrypt information when government wants to spy on you, there is no guarantee of what the future may hold. There have been bills introduced, for example, which would have made it a crime to wear body armor when government wants to shoot you. That is, if you were to commit certain crimes while wearing a Kevlar vest, then that fact would constitute a separate federal crime of its own. This law to my knowledge has not passed ... yet ... but it does indicate how government thinks.

Other technological applications, however, do indeed pose legal isks. We recognize, for example, that anyone who helped a pre-Civil War slave escape on the "underground railroad" was making a clearly illegal use of technology - as the sovereign government of the United States of America at that time found the buying and selling of human beings quite as acceptable as the buying and selling of cattle. Similarly, during Prohibition, anyone who used his bathtub to ferment yeast and sugar into the illegal psychoactive drug, alcohol - the controlled substance, wine - was using technology in a way that could get him shot dead by federal agents for his "crime" - unfortunately not to be restored to life when Congress reversed itself and re-permitted use of this drug.

So ... to quote a former President, un-indicted co-conspirator and pardoned felon ... "Let me make one thing perfectly clear:" The LiberTech Project does not advocate, participate in, or conspire in the violation of any law - no matter how oppressive, unconstitutional or simply stupid such law may be. It does engage in description (for educational and informational purposes only) of technological processes, and some of these processes (like flying a plane or manufacturing a firearm) may well require appropriate licensing to perform legally. Fortunately, no license is needed for the distribution or receipt of information itself.

So, the next time you look at the political scene and despair, thinking, "Well, if 51% of the nation and 51% of this State, and 51% of this city have to turn Libertarian before I'll be free, then somebody might as well cut my goddamn throat now, and put me out of my misery" - recognize that such is not the case. There exist ways to make yourself free.

If you wish to explore such techniques via the Project, you are welcome to give me your name and address - or a fake name and mail drop, for that matter - and you'll go on the mailing list for my erratically-published newsletter. Any friends or acquaintances whom you think would be interested are welcome as well. I'm not even asking for stamped self-addressed envelopes, since my printer can handle mailing labels and actual postage costs are down in the noise compared with the other efforts in getting an issue out. If you should have an idea to share, or even a useful product to plug, I'll be glad to have you write it up for publication. Even if you want to be the proverbial "free rider" and just benefit from what others contribute - you're still welcome: Everything will be public domain; feel free to copy it or give it away (or sell it, for that matter, 'cause if you can get money for it while I'm taking full-page ads trying to give it away, you're certainly entitled to your capitalist profit ...) Anyway, every application of these principles should make the world just a little freer, and I'm certainly willing to underwrite that, at least for the forseeable future.

I will leave you with one final thought: If you don't learn how to beat your plowshares into swords before they outlaw swords, then you sure as HELL ought to learn before they outlaw plowshares too.

Chuck Hammill

THE LIBERTECH PROJECT
3194 Queensbury Drive
Los Angeles
California 90064
USA

Subscriptions free for the asking.

(Ed: We cannot guarantee the permanence of the above organisation or address, but as of 1992, we are told, it still applies.)