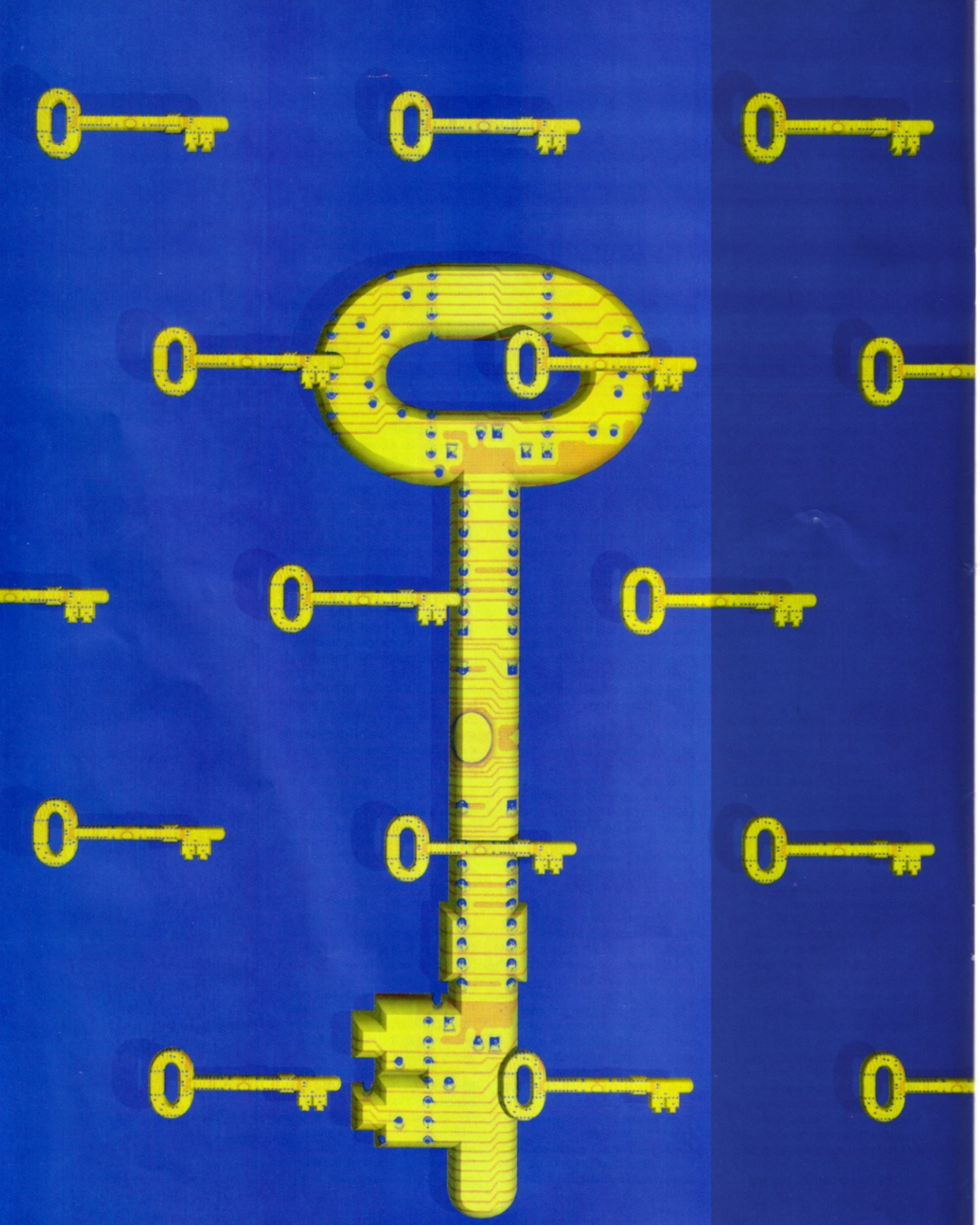
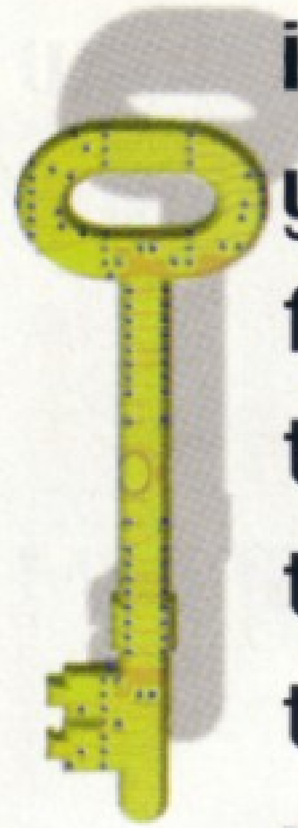


Tales From The Crypt

So once you're in the Internet and communicating digitally, how do you stop other people (like governments or big corporations) scanning through your private business? We managed to decrypt this report from MATTHEW GREAM & ROSIE CROSS...

Cryptography, huh? Never heard of it? Well, next time you're at Pizza Hut, check out some of the games provided on the placemats they give out to keep you happy whilst you wait for your pizza. You might find the same system once used by Julius Caesar now masquerading as a challenging little "break the code" puzzle. To you, this may seem like a bit of harmless fun, but the real life game of code making and breaking is deadly serious.

Whether you realise it or not, cryptography – the methods used for secret communications – is part of many everyday »»



utilities you use, one of which involves the PIN number you need to unlock cash from the bank. Unfortunately you won't be able to break these modern systems with a pencil and paper while fuelling up on pizza but you have tasted the ease with which these early systems, which were considered difficult in their day, have been cracked.

In fact, most of us, although baffled by the mathematical complexities of cryptography, key escrow, finite fields and provable complexity, would only need a few hours and a good supply of pencils and paper to crack nearly all of the systems used up to and during World War Two. During and after WW2 we saw the exponential renaissance of machines. Computers began to revolutionise our ability to play with and manipulate numbers and algorithms. The speed with which they could chew complex relationships allowed friend and foe alike to enlist the computer as a stealthy secret agent nuking opponents with the equivalent of tonnes of invisible ink.

However, even in this post world war electronic age, the ability to intercept, encrypt and decrypt information still has vital consequences. The State continues its colossal and chilling task of tracking and scanning zillions of gigabytes of information currently being disseminated digitally.

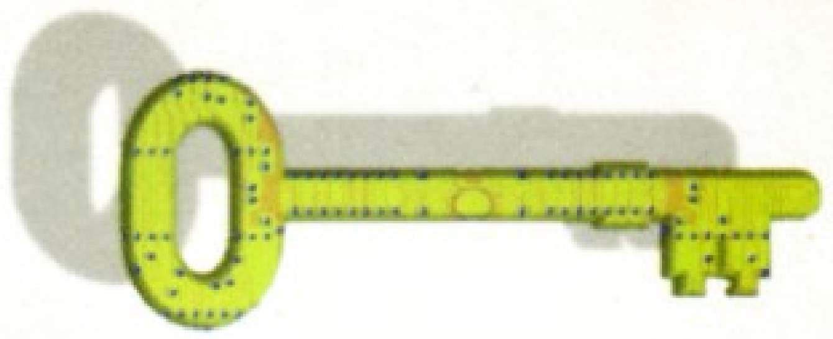
Scratching your head, and wondering why "they" bother? Because post cold war power plays have become a frenetic game in which virtual and real territories are being won and lost. The need to establish power and credibility in the new information battleground has become the virtual gangland war of the 90s. Information is the wealth generator of the future and those using our information superhighways may well be caught in the cross fire.

The salad bar of history is truly mega. As we load up on a feast of too much information rather than too little as in the past, we need to carefully pick and choose our tribes and communities. We are forced to drift to the conclusion that not everybody out there can be trusted. In the same way Alan Turing devised Colossus to crack the enigma code used by the Germans in WW2, modern day cryptologists and cypherpunks are making similar achievements in tracking the consequences of our digital rights and freedoms.

Intelligence agencies around the world work overtime ensuring diplomatic, government and military communications are secure against eavesdropping by foreign nations. These same intelligence agencies, such as our very own DSD (see box), actively monitor and attempt to decode foreign communications using antenna farms and overhead satellites. You'd be amazed how many hertz these agents suck up every day. However the crusty realities of a post cold war climate remains clear. The intelligence agencies are clearly losing their grip on the systems they once designed and implemented.

Decisions made now will direct the course and conduct of electronic networks for the future. And it's really far more important than choosing anchovies, olives or extra cheese. At last WE can choose a non-destructive weapon against invisible authorities who wish to control and monitor our communications. Imagine your pizza being delivered without a box. Never! Cryptography, is a thick secure cardboard box delivered to your door, via a friendly trustworthy delivery system, protecting your pizza from bugs and other nasties.

For more info, contact:
rx1@sydgate.apana.org,au
M.Gream@uts.edu.au
efa-info@iinet.com.au
PGP 2.3a, the latest version., for most types of computers is available from local BBS or FTP sites on the Internet.



How It Works & Where To Get It

The Internet is growing at a tremendous rate. More and more users log on every day. The contorted topology of computer networks means zillions of gigabytes of information flow freely and openly exposed each millisecond. E-Mail traverses many networks before reaching a final destination. Apart from the boss, the snoop, or the go-get-a-life sysop, there are lots of other interested parties wanting to see your mail, and why not! In this game, if we don't insist on legal ways to protect ourselves, we're likely to end up being part of a mega marketing data base. Now before you scrunch up your Pizza Hut placemat, ask yourself "how does this affect me?"

We know the obvious, old methods of communicating are soon to be superseded. In the next few years the convenience and swiftness of e-mail will see a lot of us say goodbye to paper, ink, envelope, lick and stamp. Whereas envelopes and written signatures served to ensure both privacy and authentication in this physically tangible domain, cryptography provides the envelopes, stamps and signatures for a digital world.

In a translucent domain of zeros and ones, cryptography acts as an electronic envelope. These are exactly the reasons Phil Zimmerman developed Pretty Good Privacy (PGP), the software system for a new age of E-mail. Electronic directories of Public-keys (see RSA box) have sprung up across the Internet to provide immediate access to another users encryption key, and hence the ability to conduct private and secure correspondence with anyone, anywhere. PGP outlets have become more prevalent than Pizza Huts.

This means big business. The National Security Agency (see the "The Prying Eyes" box) in the US, currently influences the standards, precedents and role models for the security management of other countries. The NSA treats cryptographic mechanisms with hostility and scepticism. In the hands of "foreign powers", crypto becomes an enemy. A streetfighter of mega proportions. Australian observers have a special interest in the outcome of the US governments reasons to install Clipper Chips (see Clipper box). Law enforcement concerns may have started in the United States but they have already infiltrated the political debates in our own country.

Cryptography empowers electronic users without criminal intentions to some privacy. And as noted Electronic Frontier Foundation spokesperson John Perry Barlow, likes to suggest, "the government should stay the hell out". The EFF and our own newly established Electronic Frontiers Australia are actively campaigning to ensure our digital rights are protected and inform people they need to mobilise, now. Australian cypherpunks meet regularly on-line and off to discuss the future of cryptoware.

On-line communities are realising more and more they need to be interested in the politics of privacy issues and key debates of future computer mediated communications. We are in essence part of a revolutionary new way of life challenging the old guard now fighting for its very existence. The cryptographic battle has only just begun. Happy crypting!!!

Crypto Applications

Digital cash is a must for an electronic society where we are going to earn and spend money, but its primary role will most likely be as a transfer medium between physical systems.

A successful digital cash system may well be run by the current financial institutions. In fact, two commercial systems have only just recently opened for operation in the US and UK. These two systems work via smart cards that hold your cash in onboard memory. You can add or subtract then spend it wherever supporting terminals are located. As with physical cash, caveats apply, so that if you lose your smart card, you lose your cash. But it is possible to put a password on the card that renders it useless in another's hands.

Another cryptographic mechanism of practical importance is that of hiding information or transforming it into a seemingly benign form. Steganography, as this is called, is useful in areas where the detection of even encrypted information could be dangerous. It works in situations where someone attempts to beat an encryption key out of you so as to determine what info you're hiding.

The current popular standard of digital pictures is in a 24bit colour format called JPEG. Each pixel can be any one of 16 million colours and most of us, including the majority of computer monitors which can only show 256 colours, see two very similar colours as being the same. It is possible to change one bit in most of these colour pixels without significantly altering the look of the picture.

Steganographic software has been written to do exactly this. It takes a file and hides it in a picture by sprinkling successive bits from the file across pixels of the image, and most of the time, even if you're looking, it's difficult to tell the difference between the original and modified picture.

Prying Eyes

National security is no doubt one of the most secretive areas of government. These are information black holes, sucking everything in and putting little out.

By far the most well known, the US National Security Agency (NSA) still remains the most secretive of all US government agencies. At the same time it employs some 100,000 people and has a yearly budget in excess of US$7Bn. The NSA gathers, decrypts and analyses information while at the same time designing, evaluating and recommending secure communications equipment for the Government. It is NSA's cryptographic systems that ensure only the US president can push the little red button. All these operations make it the largest employer of mathematicians anywhere in the world.

The Defence Signals Directorate (DSD) is the Australian equivalent of the NSA. One of only a few visible uses of the DSD occurred last year with an announcement that it had co-produced an encryption system specifically for the Australian Government called SENECA. The organisation otherwise spends most of it's time supplying information to other Australian intelligence agencies and sharing secrets with the NSA.

Certain export restrictions have been defined by the US government, which means that cryptographic products are classed in the same group as guns and nuclear weapons. These restrictions are preventing the use of cryptosystems but legal challenges hope to change this situation.

They Call It Clipper

When AT&T attempted to get approval from the US government to see secure encrypting telephones last year, the NSA said 'hang on a minute, we've been working on a chip we want you to use'. This chip turned out to be called the Clipper chip, and has single handedly brought cryptography into the mainstream in the USA.

The Clipper chip is intended to sit in your telephone, so when you call someone, the two phones will inform each other who the opposite party is, then start encrypting the conversation. This may sound like a good thing, but there are several problems.

The NSA won't release any details about the encryption algorithm itself, so there is no way to verify how secure it is. The NSA say they've worked on it for 10 years or longer, but that doesn't necessarily make it any better. At the same time, there are worries about NSA planted back-doors, methods by which it could easily decrypt any phone conversation without needing the keys.

If this wasn't bad enough, the US government states that Clipper solves the problem of privacy while still allowing for legitimate law enforcement needs because of it's Key Escrow mechanism. Whenever the chip is produced, it is loaded with a key, and each half of that key goes off to two different government agencies. If at some stage law enforcement needs to decrypt your communications, they are to request (note: a warrant is not required!) the two halves from both agencies, put them together and decrypt away. There are legitimate concerns about "insider trading" of keys between departments, or government officials secretly selling off access to keys. The ironic thing is that no criminal would be stupid enough to trust the system, and would end up using another,