Pros and Cons of Cryptography

We may be at risk from snoopers spying on our electronic data or communications, or fraudsters sending us fake messages under forged names.

Cryptography is a technology that provides two capabilities, *encryption* and *digital signatures*, which could help us to counter these threats. It may be worth adopting if we feel they pose a significant risk to us.

This paper summarises the main benefits, drawbacks and costs of cryptography. The companion paper *Background to Modern Cryptography* sets out the basic principles of Public Key Cryptography, with a brief account of how we got here and where we may be going; *Implementing Cryptography* deals with the practical details of choice of software and creation and management of cryptographic keys; and there is also a *Glossary of Cryptographic Terms.*

Critical Issues

The main questions we need to answer are:

1. Do we need cryptography at all? It can prevent spies from reading confidential messages that we send. It can also tell us, provably and undeniably, who sent messages that we receive and assure us that the contents of those messages have not been tampered with in transit. But are these types of attack actual risks to us?

2. Do we require to communicate securely with people outside our own group, such as professional advisers, beneficiaries etc.? We could do this only if they were willing to take part and it would incur more cost and effort than a system just for ourselves.

3. Should we stick with e-mail communication, similar to what we use at present but with added security through cryptography; or should we consider the new social media based applications, which have significant improvements but could mean a big change to our way of working?

These questions are considered further in the Conclusions section of this document.

Benefits of Cryptography

1. Encryption

Computers are at risk from espionage. A snooper may intercept your electronic communications in transit, or gain access to your computer and read or falsify the data you have stored there; a common saying is, you should never put anything in an unencrypted message that you would not write on a postcard.

Encryption *can* protect stored data and outgoing messages against espionage, but do we need it? So far as I know, espionage has not been a problem for charities. Is there perhaps less call for secrecy in charities' affairs than in those of a commercial operation? Is the information we send or receive really confidential or of interest to an attacker; for example:

- personal information (e.g. "An outstanding undergraduate, *x*, has been offered a place at *y* starting in October");
- information concerning our financial affairs or investments; and
- Agenda Papers and Meeting Minutes?

2. Digital Signatures

Confidence tricksters may pose as contacts we trust, by sending us messages under false names, to obtain confidential information (known as *phishing*) or mislead us into ill-advised commitments. But, while some such messages may be plausible, most are given away by mistakes in grammar, spelling, facts, context or cultural references.

Digital signatures can prove who wrote incoming messages and guarantee that their contents have not been tampered with, but only if you check the signature verification reports; these are often overlooked in the flood of unsigned messages. Should we use signatures ourselves on communications that deal with subjects of critical importance or contain requests for money, and encourage our key contacts to do so too, for example:

- Professional advisers, e.g. accountants and investment managers; or
- Beneficiaries, e.g. university colleges and departments?

Drawbacks of Cryptography

Cryptography has some downsides. None are absolute stoppers: depending on what we want to do, they may not concern us; or we can take action to avoid them – though there may be a cost in doing so.

1. Correspondents Without Cryptographic Capability

You cannot communicate with someone by using cryptography unless they have the capability too. It is no use encrypting a message to them unless they are able to decrypt it. You cannot check the authorship of a message unless it is signed.

Likelihood: high. The majority of IT users including – so far as we know – our present correspondents do not use cryptography or plan to do so.

Impact: medium. If our external contacts do not have cryptography, we can make only limited use of it, within our own group.

Avoidance: difficult. We would need to persuade our correspondents to adopt cryptography. They might want us to use the *S/MIME* standard, which is popular in the corporate world but would incur additional costs for us.

2. Uncertain Direction of Travel

The 1990s implementations of public key cryptography are now becoming dated. They do not provide the ease of use that present-day users have come to expect, fit comfortably into modern styles of operation or take advantage of recent technical developments. Modern social media-based implementations solve some of these problems, but fragment the internet into separate 'walled gardens', so may add to the problem of communicating with external contacts.

Likelihood: inevitable, at least in the medium to longer term.

Impact: probably huge.

Avoidance: evaluate the new software; decide whether we want to adopt it or stick to the old for the time being.

3. Stolen or Counterfeit Credentials

A **thief** who steals your cryptographic *identity* can:

(1) send messages to your contacts, with fake digital signatures so as to look as if the messages came from you;

(2) decrypt your incoming mail (if they can intercept it); and

(3) decrypt your confidential stored documents (if they can access them).

To do this, they must gain access to your system by producing credentials:

- your *Private Key,* a secret file on your computer or mobile device that you alone should have; and

- on systems that require *two-factor authentication (2FA),* your secret *passphrase* that you have made up and memorised.

A **forger** who passes off a counterfeit Public Key as yours can send fake messages in your name as in (1) above, but would find it hard to intercept your incoming mail as in (2) above without your noticing and cannot read your stored documents as in (3) above.

Likelihood: low.

Impact: severe.

Recovery: reset your cryptography account, generate a new *key pair* for yourself and distribute your new Public Key to all your contacts. Find out whether any confidential information may have been stolen, or fraudulent communications accepted and acted on.

Avoidance: use a strong passphrase to protect the Private Key in storage and, especially, in transmission. Do not store Private Key and passphrase together, whether on paper, a computer, a mobile device or portable media. Preferably, do not transmit them via an insecure method such as WiFi or unencrypted e-mail. Check the authenticity of any new or replacement keys that you receive. *Forward secrecy* can limit the damage in the case of your Private Key being stolen.

4. Lost Credentials

If you lose your Private Key or passphrase, **the contents of stored documents (including encrypted correspondence) protected using that key/passphrase combination will be lost for ever.** Also, you will be unable to read encrypted messages sent to you, or to send messages signed in your own name.

Likelihood: medium to high.

Impact: severe if stored documents affected, minor to moderate if not.

Recovery: reset your cryptography account, generate a new key pair for yourself and distribute your new Public Key to all your contacts. **But there is no way** of retrieving your stored documents.

Avoidance: secure back-up of keys and passphrases. We could use an external Key Escrow service, or each of us could give a copy of their Private Key to one other Trustee and their passphrase to another.

5. Unattended Device

An unattended computer or mobile device may be vulnerable to accidental leakage of information or deliberate espionage. Perhaps the owner went for a cup of coffee; perhaps it was left in a pub or on a train, or dropped in the street, or stolen. If a cryptographic application is still in an active session on the device, any casual passer-by or finder may be able to enjoy all the privileges of the rightful owner; even if the device was powered off, switching it on may take it straight back into the previous session, possibly displaying confidential exchanges from that conversation on the screen.

Likelihood: moderate for desktop machine, high for mobile device.

Impact: potentially severe.

Avoidance: One way to protect the device is by locking its screen. Either the device's operating system or the application may be able to do this; the device cannot then be operated without first providing some form of authentication such as a password. Another way is to log out of the cryptographic application.

Ideally, the system or application should be set to apply one of these protections automatically after either a preset period of inactivity or device power-off, rather than relying on the user to remember to do this.

6. Lack of Transparency

Some trusts have got into trouble through misgovernance by an over-powerful Trustee who has kept their fellow-Trustees in the dark. The Mirror Group Pension Fund under the late Robert Maxwell is an example and Charity Commission investigations reveal others from time to time. Such fraudsters could use cryptography to hide the traces of their activities.

Likelihood: low.

Impact: potentially severe.

Avoidance: good operational and auditing procedures.

7. Conflict with Other Security Measures

Encrypting a message prevents any server that it passes through *en route* from sender to recipient, including the site's own mail server, from virus-checking it.

Adding disclaimers or copyright statements within digitally signed message content invalidates the signature and will be reported as suspected tampering.

Likelihood: high for virus checking, low for notices.

Impact: moderate.

Avoidance: recipients should virus-check messages after receipt, even if they are supposed to have been virus-checked by their site's mail server. If either sender or recipient's site management feel it necessary to add notices to messages, this can be done on the server provided the notice is not placed within the signed content of a message.

The Cost of Cryptography

Set-up and Administration *(per computer)*

The following are approximate measurements of time taken to set up cryptography using Gpg4win on a desktop computer running Microsoft Windows:

Operation	Time (mins)
1. Download cryptography software and check integrity of downloaded file	3
2. Install cryptography software	$1\frac{1}{4}$
3. Reboot after installing	$2\frac{3}{4}$
4. Generate key pair	2
5. Back-up key pair	$\frac{1}{2}$
6. Export public key	$\frac{1}{2}$
TOTAL	**10**

To these basic timings you should add time for:

- thinking;
- copying the key pair securely to other devices of the same *owner* (but you can offset this against the time saved by not having to generate key pairs on those devices and you can avoid it altogether by using the multi-device support provided by social media-based cryptography applications);
- distributing copies of the Public Key to *users* who need it; and
- installing copies of other people's Public Keys, received from their respective owners, for use on this owner's devices.

Set-up time for each computer or mobile device will also vary depending on the type of system being set up, the hardware on which it is being installed and the operating system under which it is running.

Day-to-day Operation

In day-to-day operation, the main differences between plain text and encrypted communication are that:

- you will be asked to enter your secret passphrase (if you have one) from time to time;
- you will need to pay attention to warnings, reported by the cryptography software, of incoming messages with invalid signatures or from unknown correspondents; and
- if you keep data and correspondence stored in encrypted form, rather than plaintext, you will need to decrypt them whenever you want to read or search them.

Hardware Costs

Old computers may need to be upgraded or replaced in order to run cryptography. This is only likely to apply to Windows XP or earlier machines. Upgrading can take hours of work for little benefit, so replacement is recommended.

Software Costs

Updates to cryptography software tend to come out quite often but costs are not high, for example:

- Gpg4win for Windows: voluntary donation, amount at own discretion; or
- iPGMail for iPad or iPhone: US$1.99 per download.

Certification Costs

If we had to adopt the certificate-based *S/MIME* standard, we would incur extra financial and administrative costs plus certification fees. S/MIME would only be required if we had a correspondent who insisted on using it for communicating with us, but it is widely used in the corporate world. We might also have to incorporate so as to obtain a corporate identity for our certificate.

Conclusions

With reference to the three Critical Issues stated at the beginning of this paper:

1. We could quite easily protect stored data and electronic communication within our own group from spying and tampering, by using cryptography. We should do it if, and only if, we judge those risks to be serious enough to justify it. The costs need not be great and we could overcome the other potential drawbacks by simple operational changes.

2. Extending this protection to communication with people outside our own group would only be feasible if they adopted it too. This does not rule it out, but could prove costly in time, money and effort.

3. The benefits and drawbacks of the new social media based cryptography relative to the original e-mail based Public Key Cryptography are discussed in the Conclusions section of the *Background to Modern Cryptography* paper.

If we think cryptography is worth pursuing, we will need to decide on the style of cryptography we wish to adopt. The companion document *Implementing Cryptography* provides guidance on standards, protocols and applications.

Richard Stonehouse