# 

# 

18 January 2016

**Cybersecurity:   
Modified Rapture**

Sir John O’Reilly

**Introduction**

Cyber Security – or rather cyber insecurity – is very much in the news. Pretty much daily we hear of another security breach with thousands, even millions, of people affected. Yet surely we have the technology to enable the IT professional community to protect us from all this, do we not?

Well that is what I want to talk about in this ‘Cook’s World Tour’ of an introductory lecture. I will start by looking at the current context – essentially through snapshots as we see the issues unfolding on screens, in newspapers, etc.

I will then pick out a few aspects of technology with the intent simply of giving a flavour of some of what is involved – both available and also perhaps about to appear over the horizon.

But I will suggest in particular that technology on its own cannot deliver the required level of cybersecurity. It is important to think of and work with the system as a whole - and the system includes people, so people and behaviours need to be factored in too.

**Networks, networks everywhere**

Let us start with the obvious.

Networks are everywhere: telecommunications and the internet as we generally think of it, of course, but much more too, ranging from air traffic control to integrated manufacturing, from control structures for the electricity supply, to remotely controlled vehicles such as drones and other UAVs (uninhabited air vehicles).

And cybersecurity is right up there as a major concern for business. It will be even more important as the ‘Internet of Things’ (IoT) – the envisaged myriad of multiple interconnected sensors and devices to be embedded throughout the fabric of society – moves from conception/aspiration to reality, with our world becoming yet more mobile and interconnected.

**Modified Rapture**

So cybersecurity is in the news – but the news is far from all good. As Nanki-Poo in Gilbert and Sullivan’s comic opera *The Mikado* put it . . . ‘modified rapture’.

Just a few headlines serve to underscore the point:

*‘Banks lose $1bn in cyber-robberies’*

*‘US Banks attacked, manipulated and left (heart) bleeding’*

*‘Cyber theft hits 1 in 5, consumers survey finds’*

*‘Black Friday: Cyber-thieves target Christmas shoppers’*

It extends beyond the financial sector *per se.* Other disturbing headlines include:

*‘Bluebox Broadband: 3,000 customers’ details published online’*

*‘AshleyMadison personal user data exposed online’*

*‘Universities steel themselves for wave of cyber attacks’*

*‘Children’s’ electronic toy maker Vtech hacked’*

*‘Pictures of children in Vtech hack’*

*‘Net firm finds unauthorised code’*

And it impacts directly on governments and Nation States too:

*‘German Parliament to turn off computers – for repair following cyberattack’*

*‘FBI seeks hacker after 1.2 billion logins are stolen’*

*‘Turkey under ‘most intense’ cyber-attack in its history’*

*‘5.6 million fingerprints stolen in US government data hack’*

*‘Australia Bureau of Meteorology hacked’*

The problem for governments is nicely captured by:

*‘Once David learns to code malware, Goliath’s in trouble’*

Yet even without malicious intent exposure can occur – mistakes will be made.

We saw just recently an announcement from AVG, the provider of a popular tool used by millions of people that is meant to ward off malware, that it contained a flaw putting personal data at risk. The security team at Google spotted that this was overriding safety features in their Chrome browser such that users’ internet history and other personal data could be seen by those who knew where to look online – and potentially exposing email and other online activity too. The problem was resolved by AVG issuing a new version of its software but it does underscore the risks. Dr Steven Murdoch of UCL commenting to BBC News put it like this:

*‘Although now fixed, it shows that almost any software installed on a computer can introduce security vulnerabilities, even if that software is intended to improve security’*

And to compound things we’ve recently seen reports of ‘ransomware as a service’. The business model involves ‘cyber-smart’ individuals with criminal intent providing via the Dark Web ‘tailor it yourself’ software tools to those less cyber-smart of similar criminal intent.

And the bad news – or rather even worse news – is that ‘the bad guys’ are getting better. Accordingly there is a growing demand for more skilled cyber security engineers – and as pointed out in *IET Engineering and Technology Reference*, they have their work cut out to keep up in this fast moving sector.

With cyber skills at a premium interesting avenues are being explored. For example, the importance of cyber skills for national security has led MI6 in the UK to look to recruiting from *Mumsnet* and also initiating a new apprenticeship scheme with a foundation degree run by GCHQ (the Government Communications Head Quarters). The skills challenge applies further afield too. For example, South Korea is offering scholarships to build up its strength in this area, concerned about hackers from further north.

The Net, of course, by its very nature is ubiquitous and pervasive; hence with the inevitably with which night follows day so is cybercrime. It knows no boundaries and affects people on a local, regional and global level. No surprise then, that governments, concerned about national security, are eager to enhance the extent to which they/their agencies can arrange to have privileged access to sites, monitor traffic, access, etc. In this context we have seen the Investigatory Powers Bill in the UK - with the proposals seen variously as both a threat to data security for individuals and companies and an assault on personal freedoms.

*“Any attempts to weaken data security to provide a digital ‘back door’ for spies would also benefit criminals. Efforts to bypass encryption technology could have ‘very dire consequences’ for consumers by making their data less secure.”*

Tim Cook, chief executive of Apple

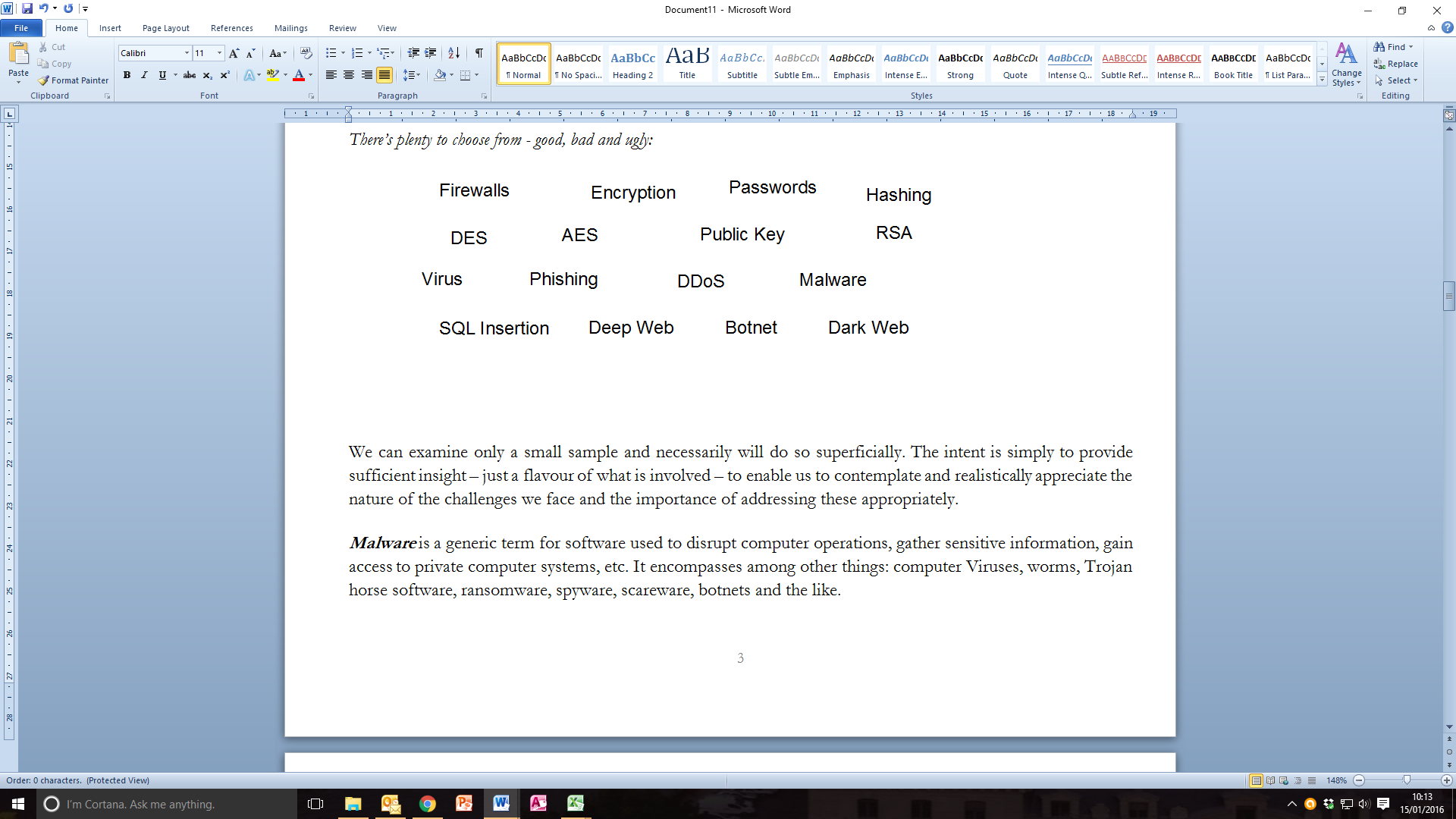
*“After all the talk of climbdowns and safeguards, this long-awaited Bill constitutes a breath-taking attack on the Internet security of every man, woman and child in our country”*

Shami Chakrabarti, Director of Liberty

**A soupçon of technology**

With that background let’s now dip our toes, albeit shallowly, into what is the very deep pool of digital security technology. There’s plenty of it out there. Much excellent work has gone into developing sophisticated schemes and arrangements helping keep use safer in ‘cyberspace’ than otherwise would be the case. On the other hand, there are a myriad of approaches, tools and techniques available and being used to circumvent cybersecurity protection arrangements – and to overcome these protections.

*There’s plenty to choose from* *- good, bad and ugly:*



We can examine only a small sample and necessarily will do so superficially. The intent is simply to provide sufficient insight – just a flavour of what is involved – to enable us to contemplate and realistically appreciate the nature of the challenges we face and the importance of addressing these appropriately.

***Malware*** is a generic term for software used to disrupt computer operations, gather sensitive information, gain access to private computer systems, etc. It encompasses among other things: computer viruses, worms, Trojan horse software, ransomware, spyware, scareware, botnets and the like.

***Cyber-attacks*** can take various forms. One example is ‘phishing’ – with ‘spear-phishing’ a variant targeting individuals with emails containing software or a link that downloads malicious software.

***Distributed Denial of Service (DDoS)*** attacks have been much in the news recently, with botnets (malicious software secreted into many computers on the Internet) sending messages/requests to overload a target system.

By way of illustration, a DDoS attack may be used to mask an attempt to steal information by overwhelming an online service with false requests, exhausting server resources (memory) and clogging ‘pipelines’ to the network. Using botnet malware and infecting clusters of cell phones, PCs or routers, provides remote control to the hacker. The DDoS attack does not breach the perimeter ‘firewall’ security but forces the IT team to mitigate damage, masking the real attack. The attack itself takes the form of malicious code (an example is an approach called SQL insertion) which tells the server to bypass authentication and retrieve customers’ bank and credit card details.

In just one sample 7 day period in 2015 more than 650,000 DDoS attacks were experienced by the top five countries taken together (in order, USA, Russia, France, India, Germany). Of these DDoS attacks almost half a million had other attacks associated with them – and a quarter of these were aimed at theft of sensitive data.

***System Protection***

So what sort of technology have we got helping or trying to keep us safe?

Most immediately familiar of course are Passwords which we experience directly as individual users. As other examples there is the evocative metaphorical term Firewall whilst underlying these and other technological devices we have Encryption.

***Password:*** *“A string of characters used for user authentication to prove identity or access approval to gain access to a resource . . . which should be kept secret from those not allowed access”*

***Firewalls*** *protect computers and networks from external attacks, controlling the data in and out. They may be installed on individual computers or on a server or router as part of the entire network. Encryption involves encoding information such that it can be read only by ‘authorised’ parties who have the ‘key’ with which to effect decoding.*

***Encryption:*** *The process of encoding messages or information such that only authorized parties can read it*

Encryption plays such a central part in cyber system security that, whilst we can’t here go into great detail, it is appropriate nonetheless to examine some of the underlying ideas and approaches. Some of the basic ideas go back a long way. Julius Caesar is known to have made use of substitution ciphers. Here the alphabet is shifted by a set number of steps, or reversed - or by using a mixture of the two it can be ‘deranged’ in a more complicated way.

By way of example let’s encode **Gresham College** by rotating the alphabet by 13 steps. The coding table has the form:

*Plain Text Alphabet:* A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

*Cipher Text Alphabet:* N O P Q R S T U V W X Y Z A B C D E F G H I J K L M

And the encoded message, the cipher text, is **Terfunz PbyyRtr.** At first sight the coded message looks like gibberish but decoding is straightforward once the coding approach and the number of steps involved is known.

An iconic example is provided by the enigma machines of 2nd world war fame. In essence enigma provided extremely complicated substitution ciphers. There were a huge number of possibilities for each letter which provided the strength of enigma. There were some quirks in the system, such as that it could never encode a letter as itself which weakened the code somewhat but of themselves these were insufficient to compromise the code to the point that the UK’s code breakers at Bletchley Park could realistically expect to break it. But break it they did. This naturally raises the question *“how did it come to be broken?”* of which more later.

Scrambling is another simple technique. Working with numbers to represent messages, as we do within computers and digital networks, we can effect ‘scrambling’ very easily by adding ‘random’ numbers to the message for transmission and subtracting these at the receiver end when we want to decode the message. Here the random sequence of digits represents the encoding and decoding key. By way of example:

***At the transmitter***

Message digits: 1 3 5 2 6 7 8

Random digits: 9 0 4 6 3 1 8

Addition gives: 0 3 9 8 9 8 6, Scrambled message

***At the receiver***

Scrambled message: 0 3 9 8 9 8 6

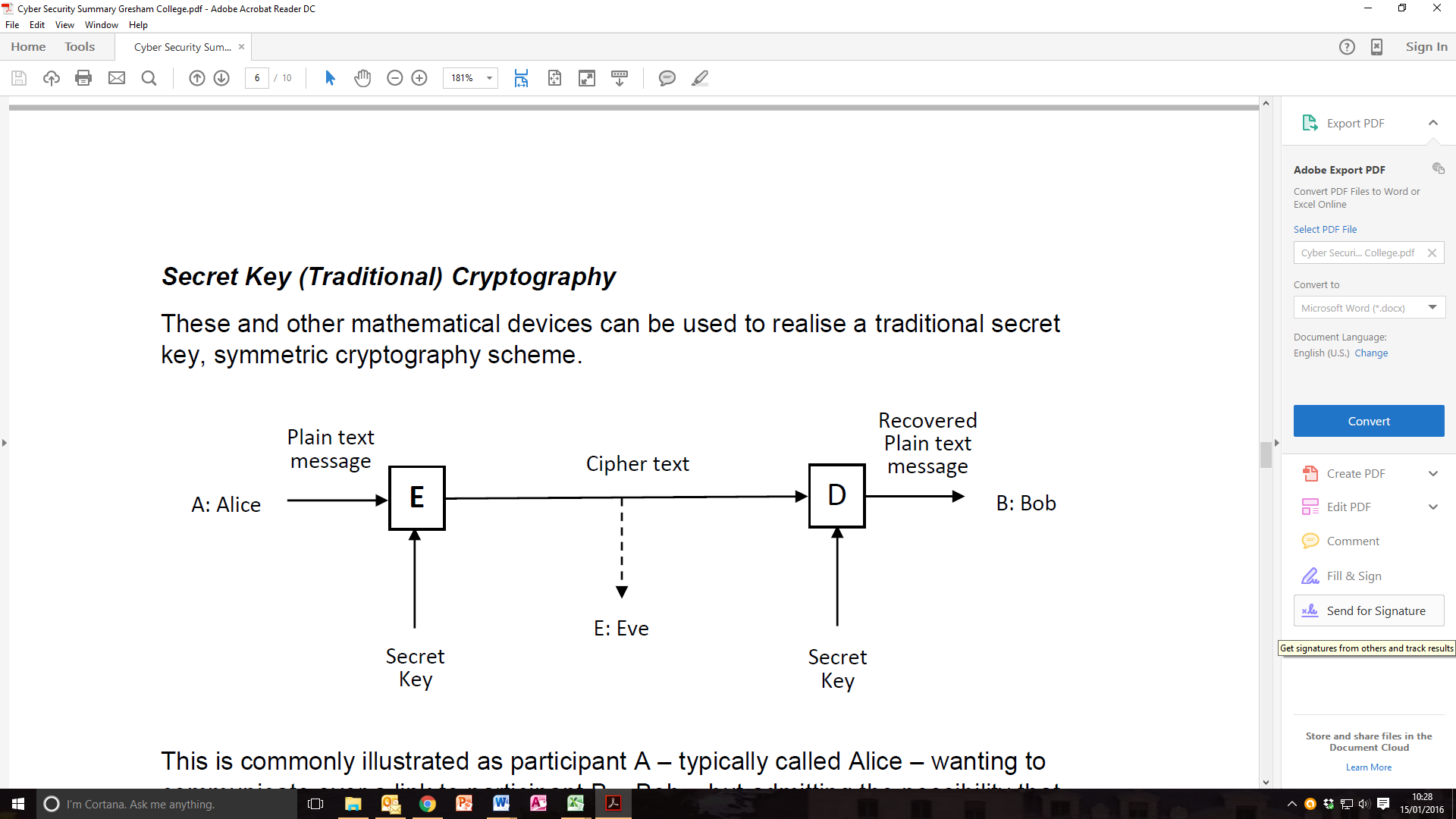
Random digits: 9 0 4 6 3 1 8

Subtraction gives: 1 3 5 2 6 7 8, Recovered ‘plain text’ message

It makes sense to do addition ‘without carries’, much as when on a 12 hour clock if it is 9 o’clock then 5 hours later we get 9 + 5 = 14 = 12 + 2 so we use the representation 2 o’clock. This is ‘clock arithmetic’ or ‘modular’ arithmetic and we say 9 + 5 = 2 (modulo 12). And of course, the principle can be applied working with number bases other than 12.

***Secret Key (Traditional) Cryptography***

These and other mathematical devices can be used to realise a traditional secret key, symmetric cryptography scheme.



This is commonly illustrated as participant A – typically called Alice – wanting to communicate over a link to participant B – Bob – but admitting the possibility that there may be an eavesdropper attempting to ‘listen in’ – that’s Eve. Provided Eve doesn’t know the secret key then with an effective encryption system it is unfeasible for it to be deduced from the encrypted message and the communication remains safe.

Cryptography based on ideas along these lines – the ‘traditional’ approach – relies on both the sender and the receiver knowing the key and it being kept secret from others. That does, though, raise the question of how the key can be secretly communicated to both parties – something of a challenge if they are at opposite ends of a network. Once the first secret key is established it can be used to distribute subsequent new keys with frequent changes of key helping keep communications secure.

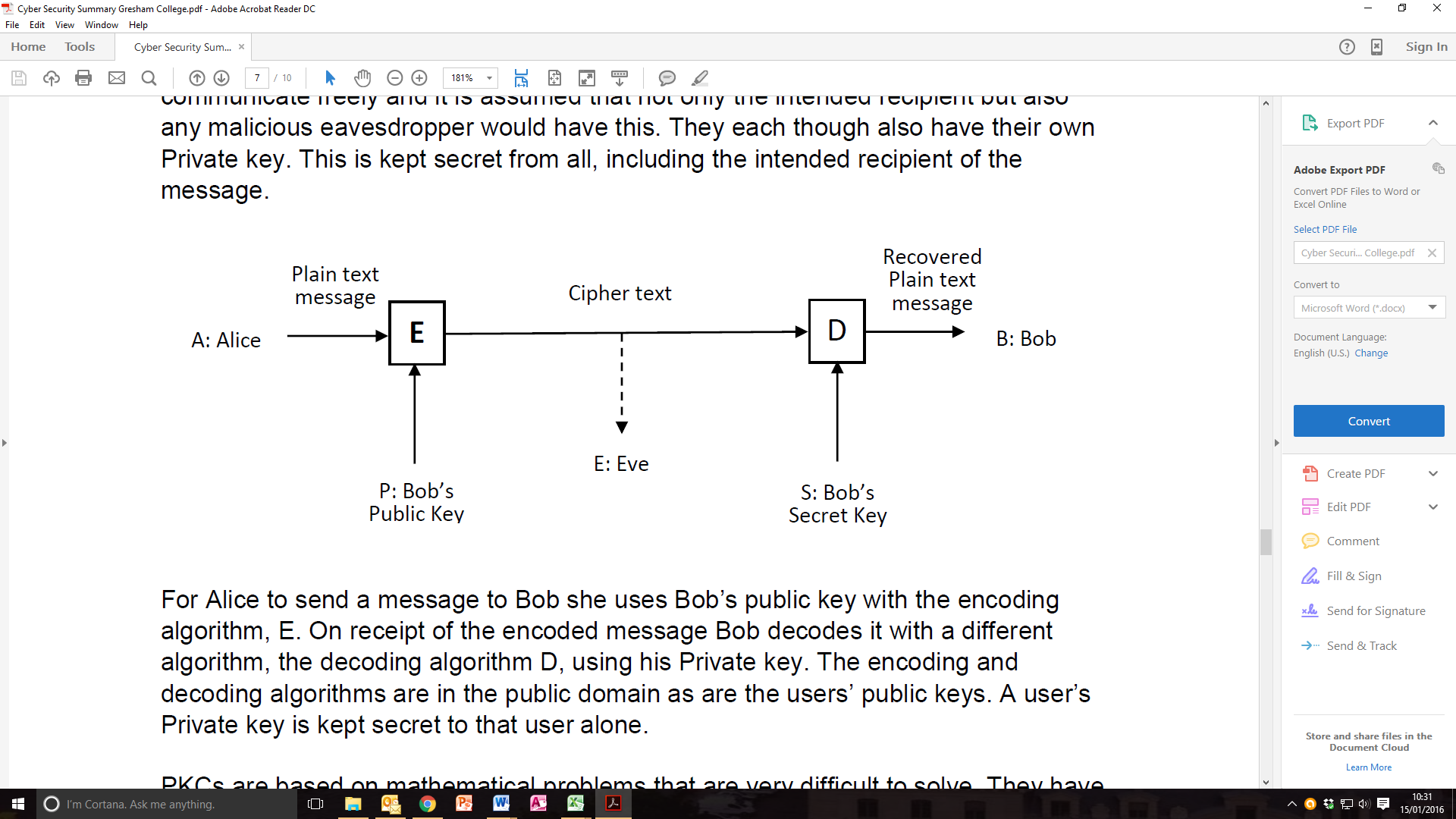
Examples of modern secret key crypto systems are DES and AES. DES – Data Encryption Standard – was formally adopted in 1977. It was known to have some potential weaknesses – along with other things that the effective key length was ‘only’ 56 bits – but was nonetheless very widely used. It was superseded in 2001 by AES – Advanced Encryption Standard. This works on 128 bit blocks of data and allows for three different key lengths: 128, 192 and 256 bits.

***A Seminal Development***

At the same time that DES was being adopted as a standard a paper authored by Whitfield Diffie and Martin Hellman appeared entitled *‘New Directions in Cryptography’*. This was a truly seminal development in that it proposed and presented a ‘proof of concept’ arrangement for asymmetric cryptosystems providing for Public Key Cryptography (PKC).

The magic of the Diffie Hellman proposal is that it allows two people to exchange a secret – such as a key for a traditional, symmetric, secret-key encryption arrangement - over a public medium without having anything shared beforehand. In outline, the steps involved are as follows. The participants first exchange some numbers (rather special and carefully chosen) over a public medium. Each then creates his/her own private number that won’t be exchanged. Also each generates his/her own public “key” using the previously agreed public numbers *together with their own private value.* Each then performs a calculation using the other’s public, own private, and the shared information - *the results match.* The result is a shared secret - a *key* for encryption produced without it ever crossing the public medium. Magic indeed!

Schematically a PKC system looks pretty similar to a secret key system but the details are very different indeed. Each user has two keys, their Public key which they communicate freely and it is assumed that not only the intended recipient but also any malicious eavesdropper would have this. They each though also have their own Private key. This is kept secret from all, including the intended recipient of the message.



For Alice to send a message to Bob she uses Bob’s public key with the encoding algorithm, E. On receipt of the encoded message Bob decodes it with a different algorithm, the decoding algorithm D, using his Private key. The encoding and decoding algorithms are in the public domain as are the users’ public keys. A user’s Private key is kept secret to that user alone.

PKCs are based on mathematical problems that are very difficult to solve. They have the characteristic that it is easy to generate a public and private key pair and to use them to effect the encryption and decryption functions but computationally infeasible for the private key to be determined from its public key counterpart. We refer to such mathematical arrangements as ‘one-way’ functions: easy to compute and very difficult (infeasible) to reverse.

You can get an idea of this by thinking of the Rubik cube – very easy to scramble it, very difficult to get it back to where you started. While the analogy is not strictly valid hopefully it serves to give the idea – and it’s not entirely irrelevant in that a cryptosystem has indeed been proposed based on Rubik’s cube.

***Trapdoor one way functions***

A function that is hard (computationally infeasible) to undo is necessary but not sufficient. There must be a device whereby, with some ‘secret’ information known only to the recipient, the proposed hard problem becomes easy. These are referred to as ‘trap door’ one-way functions. One of the first practical public-key crypto systems, based on the difficult problem of factoring a product of two very large prime numbers, is the widely used RSA scheme first publicly described by Ron Rivest, Adi Shamir, and Leonard Adleman in 1977.

As an illustration, RSA 129 involves the product of a 65 digit prime number with another prime of 64 digits yielding a composite number with 129 digits. In 1994 several computers were used in combination to factor this number – and it took some 8 months. But if one of the factors is known it is trivially simple to determine the other.

Of course, that was then and this is now; computing power has increased. In fact, if we look back it has increased dramatically as different technologies have come in, from mechanical and electromechanical, through the use of thermionic valves and then discrete transistors into the era of digital integrated circuits, realised through microelectronic fabrication. The sort of laptop that we commonly use today has the power and capability that just a few years ago would have required a very large state of the art machine. The dramatic advance has been possible through the scaling capability of silicon microelectronics. Over 5 decades and more we have seen the number of transistors per chip double about every 2 years. With the increasing density has come a similarly spectacular increase in the speed at which operations can be performed. This is reflected in the performance of computers – including ‘every day’ laptops. Alongside this, for rather different reasons, speed of data transmission has displayed similarly dramatic advances.

These advances have made it practicable to implement the very complex cryptographic coding algorithms required for secure communications – improving the cryptographic strength to combat threats. But it goes both ways, of course: at the same time the improvements in computer power are available to the hackers. So the increased computing power makes it both practicable and necessary to develop and adopt yet more powerful cyber protection schemes.

**Whole Systems, People and Behaviours**

Technology can only do so much; how it is deployed and used determines outcomes.

*“With the rise of cyber threats, specialists alone can’t defend us.”*

Ollie Whitehouse, Technical Director, NCC Group

An IT system isn’t like a castle with a single entrance and draw-bridge. It has multiple entries at different levels (multiple ‘surfaces’) – and we need to factor in people too and consider user behaviour.

The question was posed earlier ‘How did Enigma come to be broken?’ There were some aspects of the coding arrangements that represented weak points but unquestionably operating shortcomings - the way it was used – represented the dominant factor overall.

**“Operating shortcomings**

Apart from some less-than-ideal inherent characteristics of the Enigma, in practice the system's greatest weakness was the way that it was used.”

*Wikipedia*

When considering people and how they behave, it is appropriate to take note of something Samuel Johnson wrote:

*‘The chains of habit are too weak to be felt until they are too strong to be broken’*

We are all creatures of habit and it must be expected that this will play its part in the current context. Our behaviours can lead us to compromise cyber security systems. A paper highlighting this has the evocative title *‘Users are not the enemy’* exploring why users compromise systems and looking at possible remedial actions.

Indeed, users are not the enemy . . . . . . . so why do they do things like:

***Using personal email accounts for official business***

*e.g. ‘Chinese spooks may have hacked Clinton’, The Times, 12 August 2015*

***Connecting unauthorised devices***

*“Even though many organizations have policies against connecting personal smart devices to their corporate networks, employees often feel that connecting these devices via USB to charge them isn’t a problem,”*

Ken Westin, security analyst, Tripwire.

It’s not all that easy to be compliant with best practice. Just look at the problems Passwords present for users:

*“use a mixture of upper and lower case, numbers and other characters; don’t use the same password for different accounts; never write it down; change it frequently . . .’*

Perhaps this was OK in the days of a single email account – but today, when we each have 10, 20, 30 different accounts of one sort or another for which we need a password? Compliance is a real challenge. One might go so far to echo Shakespeare’s Hamlet:

*‘more often honor’d in the breach than in the observance’.*

Might technology help? This is certainly being pursued, an example being the Pico project led by Frank Stanjoy of the University of Cambridge.

There are also biometric approaches which make use of physical characteristics of individuals for identification: fingerprint, retina, iris, subtleties in the way we type and the like. Or might we make use of DNA, perhaps? Biometrics can have a part to play but should not be seen as a panacea. For example, fingerprints can be recorded and stolen; just last year 5.6 million employee fingerprints were stolen in a data breach at the US Office of Personnel Management and the DoD. Looking further ahead quantum technologies can contribute. For example quantum key distribution enables transmission of a sequence of random bits across an optical network with the laws of quantum physics showing if the sequence was intercepted or not. Beyond quantum cryptography there is the prospect of quantum computing. Significantly it has been shown how a quantum computer could perform efficient factorisation of very large numbers, reducing the time to break down RAS129 into its two constituent prime factors from months to seconds. Accordingly there is already work underway aimed at providing cybersecurity in a ‘post-quantum’ world with researches exploring algorithms not susceptible to cryptanalysis by quantum algorithms.

**Concluding Remarks**

Technology does contribute considerably, vitally, to providing cybersecurity and there is more to come. While technology advances are in train that will help further, in the meantime we should all ensure we are vigilant, make use of strong passwords, install security software and download software updates. But technology alone cannot do everything. A full system perspective and approach is necessary – and where cyber services are concerned, people and their behaviours are an integral part of the whole. Organisations must recognise the people dimension. As Matthew Aldridge of the cybersecurity company Webroot has said*:*

*‘Having a strong security policy is important, but this must be combined with awareness and training to make sure that everyone in your company understands the importance of cybersecurity’*.

**An Eclectic Bibliography**

An assembly of background reading broadly relevant to the topics addressed – some directly, others somewhat tangentially - above which may be of interest.

1. Network Security for Dummies, Chey Cobb, Pub. Wiley
2. Secrets & Lies - Digital Security in a Networked World, Bruce Schneier, Pub. Wiley
3. The Code Book, the secret history of codes and code-breaking, Simon Singh. Pub. Fourth Estate
4. The Music of the Primes, Marcus du Sautoy, Pub. Fourth Estate
5. The Man Who Loved Only Numbers, Paul Hoffman, Pub. Fourth Estate
6. On a problem of formal logic, *Proc London Mathematical Society* **30**: 264–286, (1930)
7. ‘How enigma machines work’, Louis Dade http://enigma.louisedade.co.uk/howitworks.html
8. New Directions in Cryptography, Whitfield Diffie and Martin E. Hellman, IEEE Trans. Inf. Th, VOL. IT-22, No. 6, Nov 1976
9. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Rivest, R.; Shamir, A.; Adleman, L., Communications of the ACM **21** (2): 120–126 (1978)
10. A Secure Image Encryption Algorithm Based on Rubik's Cube Principle, Khaled Loukhaoukha, Jean-Yves Chouinard, and Abdellah Berdai, Journal of Electrical and Computer Engineering, (2012)
11. Users are not the enemy, A. Adams and M. Sasse, Commun. ACM, vol. 42, no. 12, pp. 41–46, 1999
12. A Framework for Comparative Evaluation of Web Authentication Schemes, Joseph Bonneau University of Cambridge, Cormac Herley Microsoft Research, Paul C. van Oorschot Carleton University, Frank Stajanoy University of Cambridge, In Proc. IEEE Symp. on Security and Privacy 2012 (“Oakland 2012”)
13. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, PW Shor, *SIAM Journal of Computing* **26,** pp. 1484-1509 (1997)
14. The New Quantum Universe, Tony Hey and Patrick Walters, CUP 2003
15. Post-Quantum Cryptography, Bernstein, Daniel J., Buchmann, Johannes, Dahmen, Erik (Eds.) Springer 2009
16. https://cyberstreetwise.com

© Sir John O’Reilly

Gresham College

Barnard’s Inn Hall

Holborn

London

EC1N 2HH

www.gresham.ac.uk