Encryption: what it is and why it's important

An InternetNZ discussion starter

InternetNZ


InternetNZ

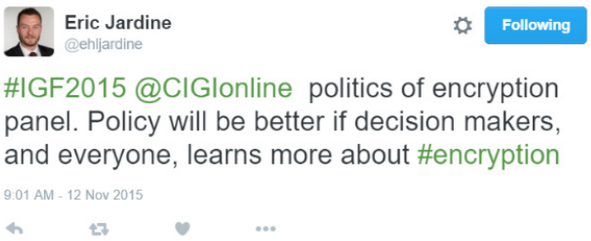
Why did we write this document?

Encryption can sound confusing, and sometimes it is. But it doesn't have to be.

In this paper we will explain what encryption technologies are, why they are useful and why they are an important part of protecting you, and your information online.

We will also cover some of the myths and current concerns around encryption being used by criminals and bad actors, why some of the recent debates about 'government backdoors' have been misguided and what some of the possible solutions really are.

At the Internet Governance Forum in November 2015, there was a panel about the politics of encryption. This tweet from Eric Jardine, who helped organise the panel, was a great summary:



We believe the politics of encryption have not improved in the last 18 months and agree with Eric that everyone would be better off if we all try to learn more about encryption, what it is and why it is useful. So, if you either:

- work in a field where you need to think about information that lives online, or is transported over the Internet
- get asked loaded questions about "terrorist use of the Internet" (or equivalent questions)
- are a guardian/kaitiaki for customer's, friend's or family's private information
- simply want to know what encryption is about but have no idea was technical terms like Elliptic Curve Cryptography are

...then this document is for you.

Contents

Why did we write this document? 1

Contents 2

Executive summary 3

What is encryption? (and why is it important?) 4

Three ways we use encryption, whether we know it or not 5

- Encryption of data at rest 5
- Encryption of data in flight 5
- End-to-end encryption 6
- What is encryption? It's a security tool 7

How important is encryption in today's Internet? 7

- Secure web connections: SSL and certificates 8
- Voice and messaging 8
- Online commerce and credit cards 9
- Encryption enables cloud and offsite storage 9
- Encryption and human rights 9
- Encryption and journalism 10
- Encryption in New Zealand 10

But people use encryption for bad as well as good 11

- Organised criminal use of encryption is commonplace 11
- Terrorist use of encryption is growing too 11
- And encryption is used digital child exploitation 11

Criminal use of encryption is making things harder for law enforcement 12

- What is happening internationally? 13

All of this has happened before: The first Crypto Wars 14

Encryption underpins trust online 15

Further reading 17

Glossary 18

About InternetNZ 19

Executive summary

Encryption technologies exist to provide privacy and security for people and businesses all over the world. Encryption technology translates data into unreadable code which is only decipherable by you and those you intend to share it with. The exact methods can differ between technologies, but typically, the receiver of this information needs to have a key to be able to decrypt the information.

Many people and organisations are using encryption as it is a vital piece of technology that brings with it a number of security benefits. It provides increased privacy and security for people and devices no matter what their intentions or goals are.

Encryption is everywhere on the Internet. Our banks use encryption technology so we're able to safely do our banking online. And e-commerce sites like Amazon and Trade Me allow us to purchase goods online without the fear of someone intercepting our credit card details. Encryption technology is also used in some messaging apps such as WhatsApp and Signal so that people can be confident that the messages they are sending are in fact private to that person only – and are not able to be read by the company that made the app, internet service providers, or any eavesdropper.

We're also seeing an increasing use of encryption by criminals and terrorists. Encryption technology helps criminals to remain anonymous and often out of sight of law enforcement. When criminals use encryption it can be difficult, or even impossible, for law enforcement to access encrypted communications or files under a search warrant. This can make it difficult to get the evidence to prosecute or secure a conviction. When terrorists use encryption it can mean that intelligence and national security agencies cannot use certain methods to detect or monitor suspicious activity.

Here lies the problem. Encryption improves our information security, but criminal use of encryption technologies create some national security and public safety risks. Encryption is not alone in this: cars, guns and baseball bats have also been used by criminals and terrorists.

This document sets out our analysis of the benefits, and risks that come with encryption.

If you want to know what we think, and our views on what some governments are seeking to "do" about encryption - then you should read our position paper "Encryption: ways forward that protect the Internet's potential." You can read this at: https://www.internetnz.nz/encryption

What is encryption?

(and why is it important?)

The following explanation of encryption is adapted from the excellent Khan Academy "What is Cryptography" course.[1]

Imagine two people, named Alice and Bob, share an important secret. For whatever reason they have had to split up but still need to communicate private information from a distance.

However, an eavesdropper named Eve also wants this information, and has the ability to intercept their messages.

So, Alice and Bob need to devise a way to communicate such that even if Eve intercepts the messages, she cannot read them. The following analogy is helpful.

First, Alice writes her message on a piece of paper and locks it in a box, using a combination lock that only she and Bob know the combination to. This is known as 'encryption.'

Then, she sends the locked box to Bob. When Bob receives the box, he can use the code that only he and Alice know, to unlock the padlock and open the box. This is called 'decryption.'

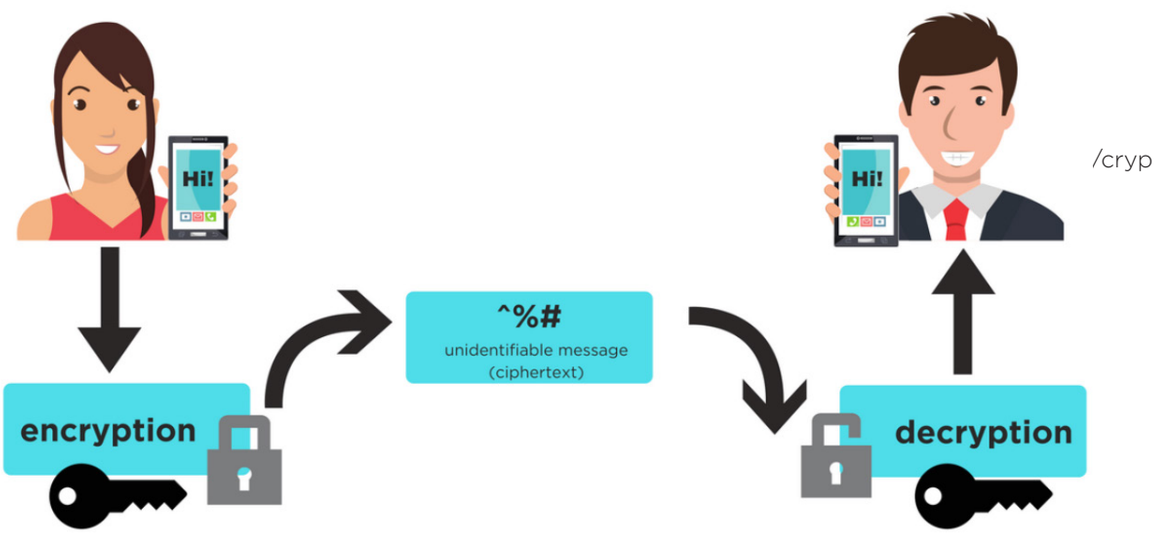
Cryptography begins when we abandon physical locks and use 'ciphers' instead. Think of ciphers as virtual locks. Ciphers allow Alice and Bob to scramble and unscramble their messages so that they would appear meaningless if Eve intercepted them.

Cryptography has been around for thousands of years. It has decided wars, and is at the heart of the worldwide communication network today.

Encryption provides us the basis for online confidentiality, ensuring that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Encryption provides for the integrity of data by ensuring that it is not tampered with, nor able to be repudiated.

It can also be used as part of authentication and authorisation systems which provide availability of data to end users.



1 /cryp

Encryption isn't one thing, it's actually three different things

Once you drill down from the very high level concept of encrypting information, it's actually useful to think about encryption technologies as three different groups:

- encryption of data while it's on a device (locking the information down when it's being stored)
- encryption of data as it's moving between computers and services (locking the information when it's moving around)
- making sure that these fit together to give you end to end encryption.

Encryption of data at rest

Storage encryption is used to protect documents and files that you have stored either in your computer or on an external drive. This often works in the background so that when you log in the data is decrypted as you access it, but when you log out the data is encrypted so anybody who gains access to your computer cannot access your information.

Examples of storage encryption include Bitlocker for Windows or FileVault for Macs.

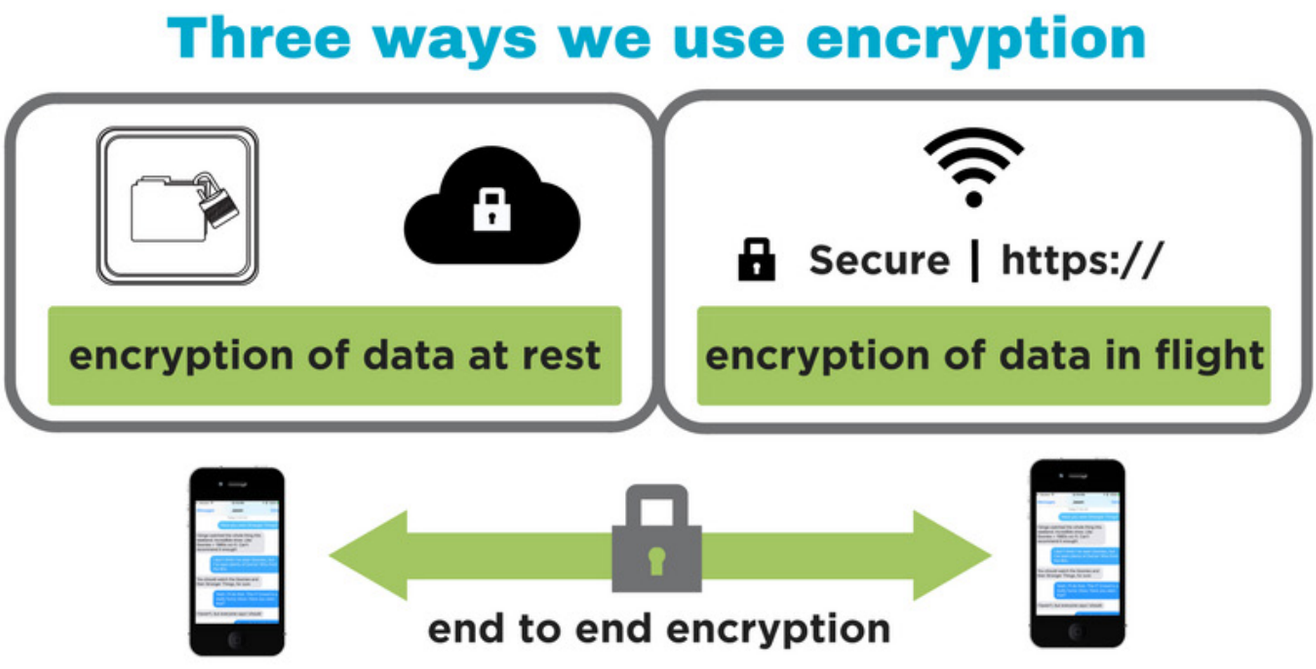
Encryption of data in flight

Traffic encryption protects your Internet traffic. It means that only you and the site or server you are communicating with can know what information is being exchanged. Traffic encryption is used to protect the transactions you make on online stores such as TradeMe, Amazon or Alibaba so that your personal information is protected from eavesdroppers. It is also used to protect your online banking details so no-one can intercept those details and steal your money.

The best known example of traffic encryption is Secure Socket Layer (SSL), which creates a private connection between your computer and a website you are visiting. You can tell when your browser is using SSL to keep your traffic secure because there will be a small padlock in front of the website address (which will begin with https:// instead of http://).

End-to-end encryption

End-to-end encryption refers to a single encryption technology that provides protection for both storage and transmission of data. One example of an end-to-end encryption technology is the Signal Protocol from Open Whisper Systems, used by a number of messaging apps (including Signal and WhatsApp). This technology encrypts messages on your phone as you write them and they remain encrypted as they are sent and are only decrypted on the phone of the person you are communicating with.



What is encryption? It's a security tool

Encryption technologies exist to provide privacy and security. As a security tool it increases the security of the system or information that you are encrypting. Most people will know about the confidentiality aspects of encryption. However, some people are not aware encryption is also useful for authentication, non-repudiation of activity and integrity.

Security dimensions of encryption*

Authentication	When using encryption we can be confident that someone is who they say they are (e.g. PGP keys for secure email), or that a server is indeed the correct one (e.g. SSL cert).
Non-repudiation	Encryption technologies can help prove someone did a thing, at a particular time. Ensuring that someone cannot refute their actions is critical to online commerce.
Confidentiality	Encryption prevents both stored information and communications from being read by anyone else. This confidentiality of information can be very useful on public networks (like the Internet).
Integrity	Encryption enables you to verify that the content of a message has remained intact or that sensitive information you have stored has not been modified after its creation, or since your last changes.

*** from OWASP Guide to Encryption https://www.owasp.org/index.php/Guide_to_Cryptography#Cryptographic_Functions**

As you can see, encryption technologies have a number of security benefits, and are not as negative for security as some think they are. It provides increased privacy and security for people, no matter what their intentions or goals are.

How important is encryption in today's Internet?

The 2015 World Internet Project New Zealand[1] suggests 42% of consumers have concerns about online intrusions into their privacy by companies and governments. Encryption is one of the most important ways with which we can ensure that our privacy is protected as we go about our lives online. Encryption is used all over the Internet with modern laptops and phones having encryption options or, in many cases, encryption built in by default.

"It's easy to see how encryption protects journalists, human rights defenders, and political activists in authoritarian countries. But encryption protects the rest of us as well. It protects our data from criminals. It protects it from competitors, neighbors, and family members. It protects it from malicious attackers, and it protects it from accidents."[2]

1 See http://icdc.aut.ac.nz/home/projects/world-internet-project

2 Bruce Schneier, https://www.schneier.com/blog/archives/2015/06/why_we_encrypt.html

Secure web connections: SSL and certificates

Roughly 50-70% of web traffic in 2016 was encrypted with secure socket layer (SSL) technology.

Websites that use SSL make it safer for you to share personal or sensitive information with them. Over the last two years, there has been an increased push to implement SSL for as many websites as possible.

SSL alone can't solve all the security or safety issues that come with browsing the web. But establishing secure connections is an important method of encryption that supports increased security, privacy and greater confidence in correctedness of information being displayed.

Voice and messaging

Voice and messaging is one area where using end-to-end encryption is really easy. We recommend using the WhatsApp and Signal private messaging apps. You can also use iMessage, but that's only secure if the person you are messaging has an iPhone (which is the same scenario as Facetime).

That's why we recommend WhatsApp and Signal to ensure that you are sending secure, private messages, regardless of what type of phone your friends or family have. Both of these apps have voice calling as well as messaging functions.

You can view our secure messaging resources at internetnz.nz/myprivacy

Online commerce and credit cards

The online banking and transactions of New Zealanders relies on encryption to ensure that no one else can uncover your banking information or steal your money while you are using your bank's website or making a purchase online.

We are sharing account information in the form of usernames and passwords, credit card information, phone numbers and addresses. All of this information needs to be protected when trading on TradeMe, buying off MightyApe, NZSale, 1Day or online grocery shopping. If it were not protected, then it would be a much simpler matter for someone to access this information and use it for potentially fraudulent purposes.

Encryption technologies mean that you can safely share payment and personal information online without someone else being able to see it.

Encryption enables cloud and offsite storage

Being able to store information in the cloud has opened up a great number of innovation opportunities. There are upsides to not having to buy and store data onsite, but there are similarly a number of downsides. You have to trust that your data is kept as confidential as it would have been on your own premises. You also have to trust that when your data journeys back and forth from the cloud that it's not changed or intercepted along the way. Encryption is an important part of giving you that peace of mind and trust. Using encryption right, in partnership with a cloud provider, means you can have more confidence in the confidentiality and integrity of the information you store in the cloud.

Encryption and human rights

Encryption protects our human rights. For dissidents, activists, media and members of the LGBTQ community encryption is a critical tool to enable them to have their privacy, communicate, collaborate, build a sense of community and explore who they are (and who they want to be).

Tools like TOR are not just used by criminals and terrorists. In fact, TOR was created to help people living under authoritarian regimes access the Internet and content they are otherwise blocked from accessing.

Encryption technologies are used to protect our privacy, freedom of association, freedom of expression, explore information to support our freedom of thought, enable the manifestation of religion and beliefs and to protect our privacy. These rights and these values are foundations of our society - foundations encryption helps to protect.

Encryption and journalism

Encryption is becoming more and more important for journalists and the news. Journalists want to protect their sources, which increasingly means using encryption to provide secure file transfers. Journalists often publish information and links to ways people can contact them without being identified.

Now, in 2017, with the current threat of 'fake news,' encryption can help news companies and journalists ensure that their readers are actually seeing unaltered stories. Political blog FiveThirtyEight recently implemented SSL, pointing out it "protects privacy and ensures readers get unaltered versions of our stories."

Encryption in New Zealand

As we've already covered, encryption technologies are used all across New Zealand. Encryption is critical for:

- keeping online commerce secure
- online identity verification
- the success of the Government's Better Public Services Result 9 and Result 10[1] which are the New Zealand public service's goals to provide online services to businesses and New Zealanders.

The offering of government services online requires robust encryption to ensure confidentiality, integrity of information provided, assurance that it is from the right source (e.g. your tax information really is from the correct source and not from a tax fraudster) and safe and secure storage of sensitive information.

We hear the occasional mention out of government circles of 'terrorist use of the Internet,' and some in our law enforcement agencies are definitely concerned about 'going dark,' which means being unable to intercept and read messages exchanged by suspects. But to date, there have not been concerted pushes from New Zealand government agencies to ban or limit encryption technologies.

Encryption is vital to New Zealand's economic prosperity and future. As a small nation at the edge of the world, New Zealand businesses need to travel far and wide to reach markets for our goods and services. Encryption helps to protect our growing intellectual property, medical and personal information (regardless of where it is located).

1 Better Public Services Results 9 and 10. http://www.ssc.govt.nz/bps-interaction-with-govt

But people use encryption for bad as well as good

One of the major technology debates of the last two years has been about the increasing use of encryption by criminals and terrorists.

Organised criminal use of encryption is commonplace

Criminals, especially organised crime groups, are sometimes at the forefront of technology use. When new technology becomes available, some criminals figure out how it can help them commit crime, make money and/or stay out of jail. In this sense, encryption is no different to cars, baseball bats, drones, computers, the Internet or ski-masks.

Encryption is effectively an everyday item that is being used for crime. It's not mostly used for crime, but we cannot ignore that it is being used for crime and encryption is generating headaches, and concern, in law enforcement agencies.

Criminal use of encryption can mean that when police officers get a search warrant, they may not be able to access encrypted communications, or files, making it difficult to get the evidence to prosecute or secure a conviction. When terrorists use encryption it can mean that intelligence and national security agencies cannot use certain methods to detect or monitor some communications.

For example, criminals trying to commit credit card fraud have taken to using Tor (a free software that prevents people from learning your location or browsing habits) to connect to banks, online trading platforms or anywhere they can commit refund-fraud. Ransomware, where criminals encrypt all of the files and documents on a computer then extort money for the decryption keys, would not be a viable business model without robust encryption technologies.

Terrorist use of encryption is growing too

Terrorist groups do use encryption technologies. They use encryption for information that is physically couriered. They use encrypted communications, and when recruiting new members, ISIS will at some point direct prospects away from plain text communications to encrypted channels.

And encryption is used in digital child exploitation

The worst types of criminals, including those who create, share and trade digital child exploitation material online, use encryption technologies. These groups heavily use device encryption, communications encryption, end-to-end encryption technologies as well as anonymity services like Tor and Tor hidden services to avoid detection and investigation by law enforcement.

Criminal use of encryption is making things harder for law enforcement

The Centre for Strategic and International Studies has identified four trends that have been driving changes to the way encryption is used and deployed online.

a. Device manufacturers and mobile developers are increasingly implementing end-to-end encryption.

b. Companies are putting in more robust methodologies to authenticate the encryption they are using, providing greater communication integrity.

c. More and more communication content is ephemeral - Snapchat, Facebook Messenger, even Signal now all offer options for automatically deleting messages after certain periods of time.

d. Finally, organisations are increasingly turning these protections on by default.

These trends combined mean that sometimes, when law enforcement seek access to a device to search for evidence, they are unable to get into the device. When terrorists use encryption it can mean that intelligence and national security agencies cannot use certain methods to detect or monitor communications.

The potential public safety consequences of criminals using encryption should not be dismissed. Example cases frustrated by encryption include:

a. In 2015, there were 11 wiretap cases in the USA (out of 4135) where unrecoverable encryption thwarted a court order.

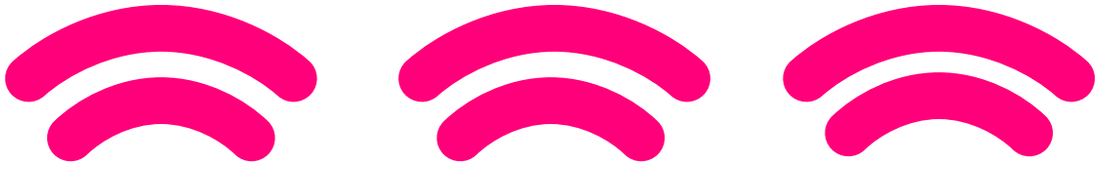
b. The New York District Attorney has some 423 seized phones that cannot be accessed.

c. The FBI took legal action against Apple to force them to unlock an iPhone 5C that was used by a gunman in San Bernadino (this case was resolved when the FBI paid a third party to hack the phone).

d. The terrorists who attacked Paris in November 2015 used a mix of burner phones, anti-surveillance tradecraft and encrypted communication and information to plan and coordinate their attack.

The lack of technical access to communications and information where there is a legal authority to gain access (either through interception or copying of information) is referred to as ‘going dark’ by law enforcement and surveillance agencies.

Some countries and law enforcement organisations are concerned enough about going dark to be taking steps to address the negative consequences of ubiquitous encryption.



What is happening internationally?

The FBI taking legal action against Apple, mentioned earlier, led to a big divide in opinions with hard stances either for, or against, strong device encryption being taken by technologists and law enforcement agencies across the world. The FBI has been collecting statistics on how often they are thwarted by device encryption with a view to having a United States national conversation about encryption in 2017.

France and Germany's governments have called for an international treaty on encryption, requiring guaranteed access to content by law enforcement and surveillance agencies. Recently, the UK Home Secretary has called on WhatsApp to turn off its end-to-end encryption by default. Russia also requires government access (aka backdoor entry), as does India.

However, what many of these governments don't seem to consider or recognise is the negative security impacts these policies create. They appear to be only thinking about national security issues without realising that one consequence of their policies is weakening the technical security of millions of citizens and businesses. As we have set out in this document, encryption is vitally important for the technical security of the modern Internet and many of the online services that we take for granted. Thinking about encryption through a narrow national security lens is dangerous and we need to think about the whole picture.

All of this has happened before: The first Crypto Wars...

This is not the first time that law enforcement and technologists have clashed over commercial and public use of encryption technologies. In the 1990s the United States Government and technology sector fought what has come to be called the Crypto Wars. As public key cryptography based encryption technologies became more available, some parts of the United States Government became concerned about law enforcement's ability to access communications it had warrants for. The Open Technology Institute, a United States technology think tank, has published a very good summary called Doomed to Repeat History: Remembering the First Crypto Wars.

"The act that truly launched the Crypto Wars was the White House's introduction of the 'Clipper Chip' in 1993. The Clipper Chip was a state-of-the-art microchip developed by government engineers which could be inserted into consumer hardware telephones, providing the public with strong cryptographic tools without sacrificing the ability of law enforcement and intelligence agencies to access unencrypted versions of those communications. The technology relied on a system of 'key escrow,' in which a copy of each chip's unique encryption key would be stored by the government.

Although White House officials mobilized both political and technical allies in support of the proposal, it faced immediate backlash from technical experts, privacy advocates, and industry leaders, who were concerned about the security and economic impact of the technology in addition to obvious civil liberties concerns. As the battle wore on throughout 1993 and into 1994, leaders from across the political spectrum joined the fray, supported by a broad coalition that opposed the Clipper Chip. When computer scientist Matt Blaze discovered a flaw in the system in May 1994, it proved to be the final blow: the Clipper Chip was dead."

Encryption underpins trust online

This document provides a short overview of how important encryption is for the Internet in the 2010s. And as you can see, encryption underpins much of today's Internet. It helps us see correct information, it increases reliability of information, ensures greater privacy for our communications and it increases the technical security of websites, devices and information.

Here is an example of the number of ways encryption is used every time you use the Internet.

Alice sits down at a local cafe, she takes out her laptop and unlocks the screensaver.[1] She joins the WiFi network[2] that the cafe provides to customers. Alice is planning an overseas trip with some friends and is trying to book some travel online. She logs into her webmail[3] using credentials stored in her password locker[4] to check the dates that her friends have already agreed upon. She remembers that they were possibly going to extend by a day or two, luckily Bob is online and she has a quick instant message conversation[5] with him to confirm. Alice logs into her favourite budget travel website.[6] She retrieves the booking she has been working on,[7] makes the last minute changes and hits purchase. The site redirects her to a secure ecommerce site to process her credit card details.[8] Finally, she is emailed[9] a confirmation of the booking which she forwards onto her equally excited friends.[10]

In that short example of doing things online, we count ten examples of encryption being used, or where we would expect encryption technologies to be used.

1. Alice's laptop (like most modern PCs) has full disk encryption enabled. When it's locked the hard drive is encrypted so that if it's lost or stolen no one can access any of her files.

2. The WiFi network in the cafe is using encryption to protect customer privacy. A password is provided to customers when they make a purchase. Here, encryption is used to ensure that only authorised customers are allowed to use the network.

3. Alice's webmail is secured with not only a username and password, but also a second factor of authentication, a cryptographically generated series of six constantly changing numbers which appear in an app on her phone. Encryption algorithms ensure that only Alice's phone and the webmail provider are able to guess the next set of numbers.

4. Alice uses a username and password stored in a cryptographically secured password locker. This is encrypted on her laptop as well as synced to other devices. The locker uses encryption to ensure that only Alice can read her own passwords.

5. Alice and Bob communicate using the Signal instant message network. Signal uses end-to-end encryption technology to ensure that no one is able to intercept or change messages between Alice and Bob.

6. Once again, Alice uses login details stored in her cryptographic password locker. Because all Alice's passwords are stored in her locker, they can be complex and unique for each website she visits. No 'alice1234' passwords for her but much more secure ones like 'correct-horse-battery-staple.' Just because Alice is careful about her logins, doesn't mean that all the sites she visit are as careful. We would hope that the website is using SSL when people make travel bookings. Looking for the https:// in the URL bar of the browser is a good hint here.

7. Similarly, we would hope that Alice's draft travel plans (possibly containing the passport numbers and personal details of her friends) are stored in an encrypted fashion by the website.

8. When Alice finally comes to make a purchase, rather than sending her credit card to the travel website, they are doing the right thing by redirecting her to a card merchant (paypal or similar) who use payment card industry data security standard (PCI/DSS) guidelines to ensure that her card data is transferred and stored in an encrypted form. The last thing Alice wants is someone stealing her card information and spending all the money she should be using for the trip.

9. It's possible that when the travel website mails out the confirmation that it uses SSL/TLS to encrypt the email as it sends it to Alice's webmail provider. This would mean that it's encrypted as it travels across the Internet, ensuring that no one in the middle could see Alice's travel plans.

10. Alice's webmail provider uses SSL encryption when it sends Alice's travel companions a copy of the email.

As you can see, even a simple everyday Internet interaction has quite a number of places where encryption is used to provide security and privacy benefits to users.

Further reading

For those of you that are really interested in this, here are some documents we think are useful and interesting when thinking about encryption and the security vs security trade-off.

Encryption: ways forward that protect the Internet's potential
InternetNZ
https://www.internetnz.nz/encryption

A worldwide survey of encryption products
B. Schneier, K. Seidel, and S. Vijayakumar
https://www.schneier.com/academic/archives/2016/02/a_worldwide_survey_o.html

DON'T PANIC, making progress on the 'Going Dark Debate'
Berkman Center's Berklett Cybersecurity Project, Harvard
https://cyber.harvard.edu/pubrelease/dont-panic/

Doomed to repeat history? Lessons from the Crypto wars of the 1990s
Open Technology Institute (New America)
https://na-production.s3.amazonaws.com/documents/Doomed_To_Repeat_History.pdf

The effect of encryption on lawful access to communication data
Jim Lewis and others. CSIS
https://www.csis.org/analysis/effect-encryption-lawful-access-communications-and-data

GOING DARK, GOING FORWARD, a primer on the encryption debate
US House of Representatives Homeland Security Committee majority staff report
https://homeland.house.gov/wp-content/uploads/2016/07/Staff-Report-Going-Dark-Going-Forward.pdf

The Elephant in the Room: Addressing Child Exploitation and Going Dark
Susan Hennessey
http://www.hoover.org/sites/default/files/research/docs/hennessey_webreadypdf.pdf

Keys Under Doormats: mandating insecurity by requiring government access to all data and communications
Ableson, Anderson, Schneir et al
https://www.schneier.com/academic/paperfiles/paper-keys-under-doormats-CSAIL.pdf

Glossary

Elliptic Curve Cryptography ECC is a type of encryption where the cryptography uses the algebra from elliptic curves, instead of fixed number.

Going dark A scary sounding term used to describe when law enforcement agencies have the legal authority to access information or a device, but do not have the technical capability to decrypt or access the information.

Signal Signal is a private messaging application that uses strong, end-to-end encryption.

SSL/TLS SSL/TLS stands for Secure Socket Layer / Transport Layer Security. Secure socket layer provides encrypted connections over the Internet.

WhatsApp WhatsApp is a private messaging application that uses strong, end-to-end encryption.

About InternetNZ

InternetNZ's vision is for a better world through a better Internet. We promote the Internet's benefits. We protect its potential. And we focus on advancing an open and uncapturable Internet for New Zealand.

We provide a voice for the Internet in New Zealand and work on behalf of all Internet users across the country.

We are the designated manager for the .nz Internet domain. And through this role we represent New Zealand at a global level.

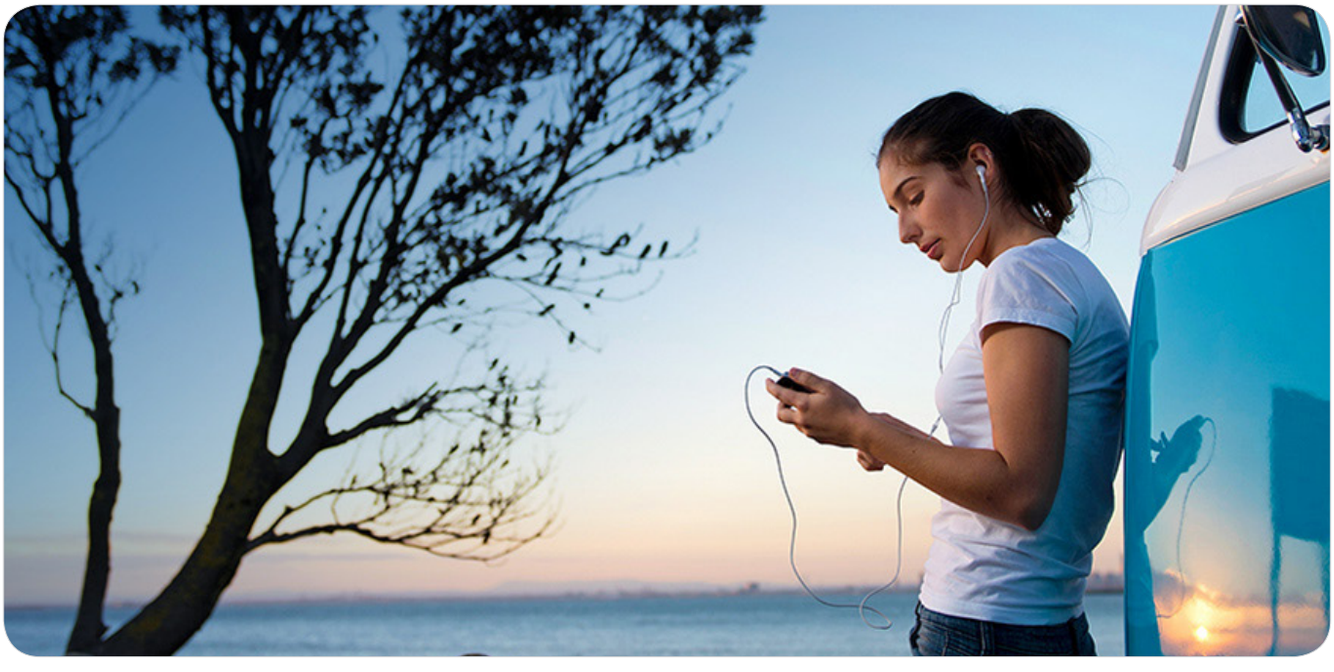
We provide community funding to promote research and the discovery of ways to improve the Internet. We inform people about the Internet and we ensure it is well understood by those making decisions that help shape it.

Every year we bring the Internet community together at events like NetHui - to share wisdom and best practice on the state of the Internet.

We are a non-profit and open membership organisation.

Be a member of InternetNZ and be part of the Internet community.

You can keep a close watch on the latest tech and telecommunications developments and network with other like-minded people at cool events. Being a member of InternetNZ only costs $21 per year. Find out more at internetnz.nz/join



InternetNZ

Level 11
80 Boulcott Street
Wellington 6011

P.O. Box 11-881
Wellington 6142
New Zealand

Free phone: 0800 101 151
Phone: +64 4 472 1600

www.internetnz.nz

@InternetNZ InternetNZ