NUTS & BOLTS *of* ENCRYPTION

A primer for policymakers on encryption

SEPTEMBER 2018

presented by:

Engine

CHARLES KOCH INSTITUTE

INTRODUCTION

Most of us use encryption every day, often without realizing it. From talking with loved ones, securing communications between Internet-connected devices, and storing and sharing sensitive health, banking, and business information, we all regularly rely on the security provided by encrypted technology.

Despite how often we use encryption—and how prominent the encryption debate has become in D.C.—few understand how it actually works. Recently, the conversation about encryption has been framed as a conflict between a select number of high profile technology companies and law enforcement, but this misses the perspective of Internet users, companies of all sizes—especially startups—and even government agencies that rely on encryption and will be impacted by any policy decisions that come out of this conversation.

That's why Engine and the Charles Koch Institute partnered on a three-panel series about "The Nuts and Bolts of Encryption" to educate policymakers and staff on how the technology behind encryption works, how it's used every day, and where the current debate over encryption stands today.

As a conclusion to this series, this report examines the concepts covered in the panels, beginning with a basic explanation of the mathematical principles behind encryption and the technical limits of those principles. At its core, encryption relies on the basic idea that it's very easy to combine two simple things into something complex, but it's very difficult to take a complex thing and separate it out into its simple components.

This report also examines several recent developments in the policy debate over encryption, including the increasing calls from law enforcement for "responsible encryption"—or having technology companies build intentional vulnerabilities into their products to provide access to data—as well as reports about law enforcement's current capabilities and impediments to accessing data in criminal investigations.

Through the event series and this report, Engine and the Charles Koch Institute hope to add context and nuance to the debate around encryption, which shouldn't be reduced to a fight between giant technology companies and law enforcement that wants access to data in times of crisis.

CONTENTS

WHAT IS ENCRYPTION?

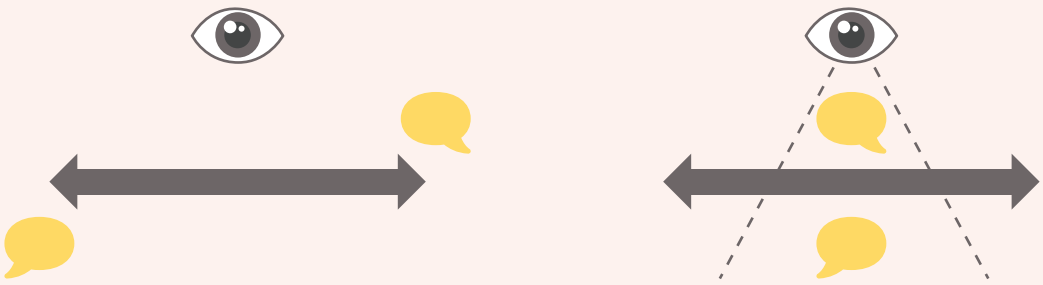
Encryption is a security tool that is used to protect data from access by unauthorized parties. Through encryption, data is "locked" and converted into an unreadable format that can only be "unlocked," or decrypted, using a specific key, which is given to or held by authorized parties.

Cryptography, or the creation and solving of codes, in its general form dates back many centuries and has been used throughout history. Ancient Mesopotamians hid trade secret information using codes while Julius Caesar used a cipher to encode military information. Since those early days, the art of hiding information using codes has advanced significantly. Today, with sophisticated computing technologies, algorithms are able to quickly generate en masse unique ways to scramble data and hide it from prying eyes.

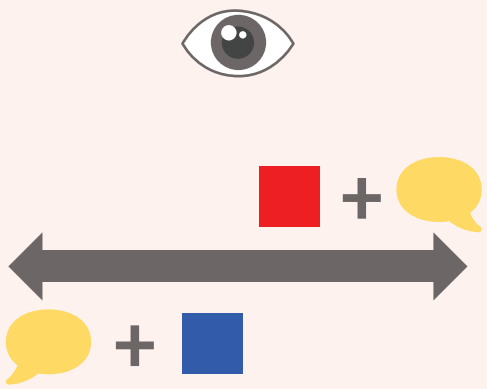
HOW DOES IT WORK?

Encryption relies on the basic idea that it's very easy to combine two simple things into something complex, but it's very difficult to take a complex thing and separate it out into its simple components.

The most common method for encrypting data relies on combining large numbers, but the concept can be demonstrated, at its most basic level, by combining primary colors.

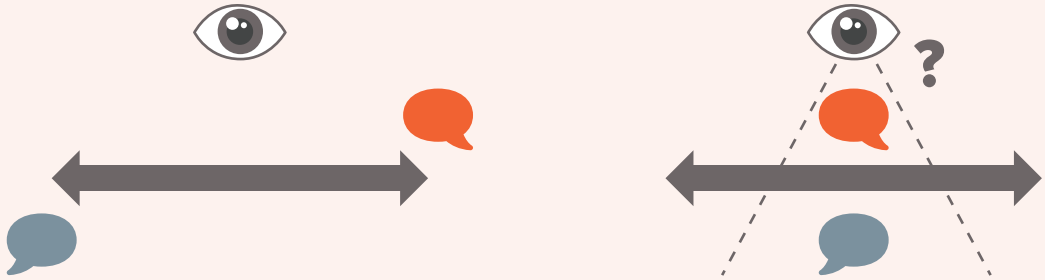


In the example above, two users are communicating over a network and through an encrypted messaging app. Each user is given two colors: yellow and either red or blue. The color yellow represents messages that are transmitted across the network in plaintext; if two parties exchange messages in their current form, a third party could easily intercept and read them.

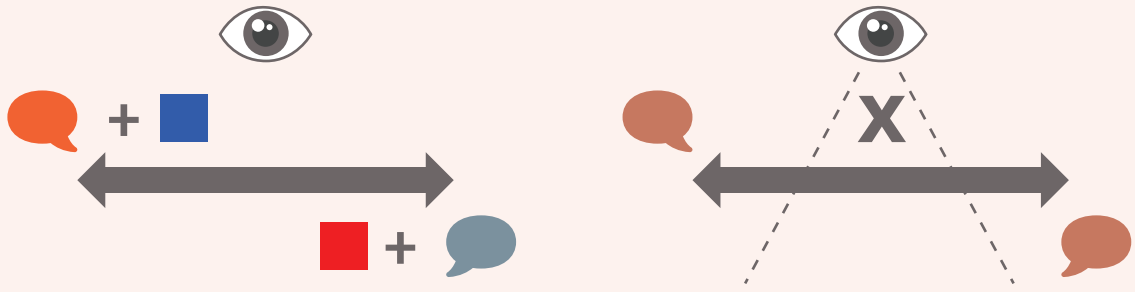


Each user can mix in a small amount of their secondary color—either red or blue—to "encrypt" the message they want to travel over the network. This represents a "private key" which belongs to an individual and is used to scramble data and protect it from unauthorized viewers. In many common encryption applications today, users don't even realize they're using a private key to protect their data, because the key lives inside the encrypted device or service they're using.

Now the colors have been mixed—or the data has been encrypted—the messages can be sent across the network without a third party understanding what they contain.



Once both parties receive the encrypted message, they have to be decrypted. To do this, each user will match the color they received with the color representing their private key. Both messages will now be "decrypted," or the same color. Since the color never passed over the network, no unauthorized third party could see the final product.



HOW DO WE USE ENCRYPTION EVERY DAY?

It is a common misconception that encryption is a complex technical process reserved for security experts and sophisticated malicious actors. Instead, encryption is increasingly integrated into our daily lives and ensures data security for Internet users, businesses, nonprofits, and governments across the globe.

Here are some of the ways in which you may be interacting with encryption technology without realizing.

Email services and messaging apps:

The technology is important to all secure online communications, including emails. Certain apps, such as Signal and Telegram, have gained a reputation purely for their robust encryption technologies.

Online transactions:

Every time you use your credit card to purchase something from a website that uses a secure protocol (HTTPS), the card number is transmitted over encrypted connections to reduce the chances of your information being stolen.

Wi-Fi connections:

If you use a password when connecting to Wi-Fi, then your connection is most likely encrypted to protect the data you transmit from interception by third parties.

Devices:

Encryption is important in a physical sense, too. For instance, computer disks which store our data are secured through a process called "disk encryption," which means that only those authorized to read the data on the disk can do so. Mobile devices, like smartphones, are also increasingly encrypted, meaning they can only be unlocked with the key, typically a passcode or biometric data like a fingerprint. This has significantly reduced the rate of smartphone theft.

RESPONSIBLE TO WHOM? AN ENCRYPTION SIMULATION

INSTRUCTIONS:

THE STORY:

You are a member of the security team at StartNet, a startup that provides network security for hundreds of platforms, websites, and applications.

The FBI has approached you because they have reason to believe that a terrorist organization is communicating using PlotChat, a chat client that runs on one of StartNet's encrypted networks. The FBI thinks terrorists are planning a potential attack using PlotChat.

You've identified specific U.S. users and traffic patterns on your network associated with PlotChat and have provided options for the FBI to get information about those users, including providing metadata about PlotChat users and communications.

Instead, the FBI wants you to build a "backdoor" into your network so that agents can intercept PlotChat messages. The agency has threatened to take you to court and a government source has leaked to the press that the FBI and StartNet are talking about building a backdoor.

THE OBJECTIVE:

In two weeks you must decide whether to cooperate with the FBI and build a backdoor into your network encryption. Before then, you'll speak with five different stakeholders and announce after each one whether or not StartNet will cooperate with the FBI. That answer will affect the number of points you have in the following three categories: User Trust, Government Cooperation, and Revenue.

Start with 30 points in each category. Every round you will make a decision which will add or subtract points in each category.

	USER TRUST	GOVERNMENT COOPERATION	REVENUE
APPROACHED BY FBI:	30	30	30
Round 1: Other Users			
Round 2: Malicious Actors			
Round 3: International Competition			
Round 4: Business Costs			
Round 5: Foreign Governments			
YOUR TOTALS:			

START

ROUND 1: OTHER USERS

You're approached by SafeHouse, a non-profit that works with domestic abuse victims. They use a chat app that runs over your encrypted networks to provide help to victims. They warn you that domestic abusers have already attempted to hack the chat app and harass victims.

If StartNet builds a backdoor, it will significantly weaken the security of the app and risk the safety of domestic abuse victims. SafeHouse will have to stop using any app run over StartNet networks, and it will publicly encourage other victims' groups to do the same.

-10 user trust
+5 government cooperation

+5 user trust
- 6 government cooperation

ROUND 2: MALICIOUS ACTORS

A major data breach is revealed at competing network security company, NotLock. Press reports revealed the company built a backdoor into its network encryption tools in 2014 at the behest of the DEA, which was investigating a drug cartel using NotLock's services.

A group of malicious hackers in the Ukraine found and exploited that vulnerability. They've intercepted and published data from NotLock's secure networks, including emails between executives at a Fortune 500 company relating to a hiring scandal.

Your clients are concerned about the risk to their businesses if StartNet creates a similar backdoor.

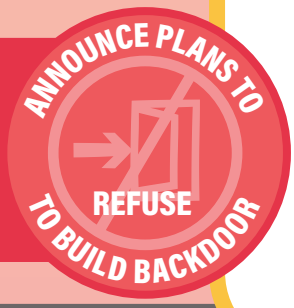
ROUND 5: FOREIGN GOVERNMENTS

A global digital rights and civil liberties group alerts you to an effort by Australian policymakers to require domestic technology companies to build intentional vulnerabilities into their products. The group warns StartNet that if it builds a backdoor for the FBI, Australian law enforcement will increase pressure on other companies to build similar backdoors into their products.

Your international compliance team warns that the costs of complying with backdoor requests from several countries will require several more engineers and international lawyers.

-10 user trust
-10 revenue
+5 government cooperation

TALLY SCORE ON PAGE 6



+5 user trust
+2 revenue
- 6 government cooperation

DECISION DAY

User Trust
If you have fewer than 20 points, StartNet will face public backlash and lose many of its users.

Revenue
If you have fewer than 15 points, StartNet will have to downsize its operations, laying off dozens of engineers.

Government Cooperation
If you have fewer than 24 points, the government will sue to compel StartNet to build in the backdoor, and the industry will face threats of legislation.

-10 user trust
+5 government cooperation

+5 user trust
- 6 government cooperation

ROUND 3: INTERNATIONAL COMPETITION

Canadian network security company MapleNet launches an aggressive ad campaign touting their break-proof encryption tools to Fortune 500 companies in the U.S. MapleNet is telling your clients that its encryption is better than StartNet's because they are outside of the FBI's reach and can't be compelled to build in a backdoor.

Your Fortune 500 clients are threatening to take their business to MapleNet.

-10 revenue
+5 government cooperation

+2 revenue
- 6 government cooperation

-10 revenue
+5 government cooperation

+2 revenue
- 6 government cooperation

ROUND 4: BUSINESS COSTS

To comply with the FBI's request and maintain reasonable network security practices, StartNet will have to either reassign several engineers or hire new engineers to build the vulnerability and then protect it from attacks by malicious actors.

Reassigning engineers would require pausing the development of new network security tools that StartNet was hoping to bring to the market later this year. Hiring new engineers will cost hundreds of thousands of dollars.

TIMELINE OF REPORTS

A lot has happened since the public debate around encryption erupted in 2015, when the FBI sued Apple in hopes of unlocking an encrypted phone tied to a mass-casualty shooting in San Bernardino, California. That legal challenge was ultimately rendered moot when the FBI found an outside company that could unlock the device. But the dispute raised lasting questions about how far companies should go to facilitate law enforcement access to encrypted data. While that question continues to be debated, several academic and news reports in 2018 have added additional context and nuance.

A proposed framework for evaluating encryption policy proposals
February 2018

CLICK TO READ MORE

In February, a new framework for considering regulatory proposals aimed at facilitating law enforcement access to encrypted data was released. The National Academies of Sciences, Engineering, and Medicine proposed a framework for considering encryption policy proposals that considered the potential impact on privacy, civil liberties of users, international law, the financial costs, and the effect on security.

Government watchdog says the FBI miscommunicated about technical capabilities around San Bernardino case
March 2018

CLICK TO READ MORE

In March, the Justice Department's internal watchdog—the Office of the Inspector General—released a report about an investigation into staff concerns that the FBI and its top officials did not accurately represent the agency's technical capabilities when pursuing legal action to force Apple to break into the locked phone tied to the 2015 San Bernardino shooting.

While the report ultimately found that the FBI's statements in court and then-FBI Director James Comey's testimony in front of Congress reflected the high-level understanding of the agency's capabilities, the Inspector General pointed to miscommunication between different FBI departments as the reason that the agency claimed in court that it needed Apple to help it access the device. The Inspector General's report stoked fears that the FBI was using the San Bernardino case to set a legal precedent that could force companies to build intentional vulnerabilities into their products to facilitate law enforcement access to encrypted data.

Government working on security through encryption, but too slowly
May 2018

CLICK TO READ MORE

In May, the administration released a mandated report on cybersecurity risks across the federal government, which found that many agencies were failing to fully use encryption to secure data.

While 73 percent of agencies have fully implemented encryption of data in transit, less than 16 percent of agencies have fully implemented encryption for data at rest, and agencies have dedicated a relatively small amount of their budgets to encryption. Securing data, including through the use of encryption, is a "low priority" for federal agencies, according to the report, despite "repeated calls" from industry, privacy advocates, and the Government Accountability Office. "It is easy to see government's priorities must be realigned," the report said.

FBI dramatically overstated the number of encrypted devices it can't access
May 2018

CLICK TO READ MORE

The Washington Post released a bombshell report in May that the FBI has repeatedly overstated by several thousand the number of encrypted devices it cannot access while conducting criminal investigations in 2017. As part of the FBI's arguments about the problems encryption poses, the agency told lawmakers and the public it cannot access nearly 7,800 locked devices. That number is actually between 1,000 and 2,000, according to the Post.

The FBI attributed the dramatic overcount to "programming errors" that occurred because it uses three databases which could cause the agency to count a single phone repeatedly. An internal estimate in May put the number of locked devices at 1,200 but the FBI said it was conducting a larger audit to determine the actual number, according to the Post.

CSIS report finds encryption outside of the top problems for law enforcement's access to data
July 2018

CLICK TO READ MORE

A survey of law enforcement agencies at the federal, state, and local levels found that lack of access to encrypted data ranked lower than several other problems that law enforcement agencies face when dealing with digital evidence. The Center for Strategic & International Studies report, "Low Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge," highlighted several obstacles faced by law enforcement, including "difficulty identifying which [companies] have access to relevant digital evidence" and "difficulty in getting relevant digital evidence from [companies] once the relevant [company] is identified."

The report also touched on the frustration that both technology companies and law enforcement feel when communicating, or miscommunicating, with each other. Law enforcement agents complained in the survey about long delays, incomplete information, and a lack of knowledge about the "magic words" that companies are looking for before they provide data to law enforcement. Companies complained about overly broad and boilerplate requests for data, as well as a lack of awareness of companies' responsibility to protect user data and privacy. The report recommended more cooperation between law enforcement and companies, including company training for law enforcement on what information is available.

The report similarly highlighted an inadequacy in overall training and resources for law enforcement to access and use digital evidence, including technical specialists, equipment, analytical tools, and legal expertise. While local and state law enforcement handles the majority of criminal investigations, those agencies are the least equipped to handle digital evidence, according to the report. Only 45 percent of local law enforcement agencies surveyed have adequate resources to access and use digital evidence, and local law enforcement agents receive, on average, just 10 hours of digital evidence training a year. The report offers recommendations to boost training and resources at the federal, state, and local levels.

GLOSSARY

At-rest encryption:
When data is encrypted "at-rest," it is being stored securely in one place, most commonly on one device.

In-transit encryption:
When data is encrypted "in transit," it is being transmitted from one party to another, usually across a network, and is protected so that it cannot be intercepted while it is moving.

Asymmetric encryption:
If encryption is asymmetric, two different keys are used to encrypt and decrypt data. This is commonly used in online services.

Symmetric encryption:
If encryption is symmetric, the key used to encrypt data is also used to decrypt data. All parties involved in exchanging the data agree upon the key before the data is encrypted.

Public key:
Asymmetric encryption (see above) uses two types of keys, one public and one private, and you need a pair comprising of each to successfully encrypt and decrypt data. A person's public key can be shared widely to allow anyone to encrypt their communications to that person.

Private key:
The closely-held key that allows a recipient to decrypt data that has been encrypted using the paired public key. The key must be kept secret to preserve the security of a system of asymmetric encryption.

Ciphertext:
After data has been encrypted, it is referred to as ciphertext. This is a disguised way of presenting the data.

Cryptography:
Also known as cryptology, this is the study of using codes to secure information.

Encryption:
The process by which data is scrambled or converted to a format unreadable by those not authorized to access the data.

End-to-end encryption (E2EE):
Communications that are encrypted end-to-end can only be viewed by the sender and receiver. No other party that may see the encrypted communications along the way—including Internet service providers, hackers, and application providers—can decrypt the communications.

Key:
A value that is the result of complex mathematical computations. This value tells the encryption algorithm how to convert from plaintext to ciphertext, and is crucial to unlocking this algorithm.

Man-In-the-middle attack:
An attack where a third party intercepts a communication between a sender and recipient. The third party might then read, or even alter, the communication before it reaches the recipient.

One-way function:
A mathematical function that can be performed one way, but not in reverse. Unlike encrypted data, which can be decrypted, once data is "hashed" through a one-way function, it cannot be "unhashed."

OTP:
A one-time-password (OTP) is a type of key that can only be used once.

Plaintext:
Data that is unprotected and has not yet been inputted into an encryption algorithm, or that is the output of decryption. Sometimes this term is used interchangeably with "cleartext" but technically speaking, cleartext refers to unprotected data that is not intended for encryption.

Session key:
A single-use symmetric key that encrypts and decrypts communications within a single use of a communications service.

In the news:
According to recent reports, the U.S. Department of Justice has asked Facebook to facilitate access to voice conversations taking place over its Messenger service, which uses session keys to secure voice calls. While Facebook is reportedly challenging the request from the Department of Justice—which came as part of a federal investigation into the MS-13 gang—encryption advocates worry that Facebook keeps the session keys for Messenger voice calls, which could be easily handed over to law enforcement.

THE CAT AND MOUSE GAME OF IMPROVING THE IMPERFECT

The math behind encryption—combining large numbers so that they can only be easily separated with the right key—is inherently inflexible. But the way companies build encryption into their products leaves room for errors, which can be found and exploited.

The efforts to improve companies' implementation of encryption is often compared to a "game of cat and mouse." As those looking to find and exploit vulnerabilities poke holes in encrypted products and services, companies must continue to anticipate and patch those holes to protect the security of their users. This is true even when the parties finding and exploiting vulnerabilities are from the law enforcement community.

Policymakers should remember that there is always someone somewhere working to find a vulnerability in an encrypted product, especially when selling those vulnerabilities can be so lucrative. A company providing an encrypted product is constantly looking to fix any vulnerabilities that could impact the security of its users.

In the news:

Most recently, the tension between these two sides has come to the fore of the encryption debate in relation to Apple devices. In June 2018, Apple introduced a "USB Restricted Mode" on its devices, which prevents data from being retrieved via the USB charging port if the phone has been locked for more than an hour, unless it is unlocked with a passcode. By doing this, Apple is preventing the lightning port from being used to gain access to information stored on the phone. That was possible before Apple introduced "USB Restricted Mode" thanks to tools sold by digital intelligence firms Celebrite and Grayshift to law enforcement and others.

Apple's move stops all unauthorized actors—whether they're hackers, identity thieves, or law enforcement—from accessing a phone that has been locked for more than an hour. Many have framed this particular issue as a confrontation between Apple and the law enforcement agencies that relied on this vulnerability to unlock encrypted phones. But when a company like Apple improves the security of its products, customers are protected from unwanted data interception from any unauthorized party. The company is simply fixing a vulnerability that could hurt the security of its users. Reducing the conversation down to a battle between the private sector and law enforcement risks ignoring the true complexity of data security, privacy, and the many stakeholders involved.

WHERE DO WE GO FROM HERE?

With cyber attacks and data leaks becoming more commonplace and high-profile, the pressure—on users, companies, and the government—to protect data is growing. As threats increase, so does the need for robust and technologically sophisticated security solutions.

The future of encryption is often questioned given the rise of new technologies, including blockchain, artificial intelligence, and quantum computing. There are specific fears that quantum computing will outpace the encryption we use today. In general, the developer community has been actively engaged in improving encryption methods to keep up with other technical advances. For instance, many large tech companies and startups are beginning to invest in quantum resistant encryption to ensure that data will be protected from attacks even if quantum computing becomes more mainstream. In other words, as technology progresses, so do the methods of security experts who are incentivized to keep innovating and improving the status quo.

The encryption debate clearly isn't going anywhere. As long as there are calls to have companies build intentional vulnerabilities into their encrypted products and services, there will be a need for a reasonable, nuanced, and fact-based conversation about how encryption works and how it's used everyday.

Engine

Engine was created in 2011 by a collection of startup CEOs, early-stage venture investors, and technology policy experts who believe that innovation and entrepreneurship are driven by small startups, competing in open, competitive markets where they can challenge dominant incumbents. We believe that entrepreneurship and innovation have stood at the core of what helps build great societies and economies, and such entrepreneurship and invention has historically been driven by small startups. Working with our ever-growing network of entrepreneurs, startups, venture capitalists, technologists, and technology policy experts across the United States, Engine ensures that the voice of the startup community is heard by policymakers at all levels of government. When startups speak, policymakers listen.

CHARLES
KOCH
INSTITUTE

For more than five decades, Charles Koch's philanthropy has inspired bold new ideas to improve American lives. Inspired by a recognition that free people are capable of extraordinary things, the Charles Koch Institute supports educational programs and dialogue to advance these principles, challenge convention, and eliminate barriers that stifle creativity and progress. We offer educational programs, paid internships, and job placement assistance to students and professionals, and encourage civil discussion about important issues like free speech, foreign policy, and criminal justice reform. In all of our programs, we are dedicated to identifying new perspectives and ideas that help people accomplish great things for themselves and others.