M2 Maths Info

2020 – 2021 – First semester

Teacher : Adrien Le Divenah

Final exam

I) Vocabulary (2 points)

RSA:

Symmetric cipher:

Distributed key:

Brute force attack:

Bonus words (1 point)

Steganography:

Frequency analysis:

II) Listening comprehension: watch this video (https://www.youtube.com/watch?v=6-JjHa-qLPk) and answer the following questions (6 points)

1) What was Caesar's cipher? Give a detailed explanation of how it works.

2) What method can you use to make that kind of encryption way more efficient?

3) Why do computers make it so hard to decipher a message without the key today?

4) Why can't we use symmetric encryption in the internet era? What's the solution then?

III) Reading comprehension (6 points)

What Is End-to-End Encryption? Another Bull's-Eye on Big Tech

By Nicole Perlroth

- Nov. 19, 2019

SAN FRANCISCO — A Justice Department official hinted on Monday that a yearslong fight over encrypted communications could become part of a sweeping investigation of big tech companies.

While a department spokesman declined to discuss specifics, a speech Monday by the deputy attorney general, Jeffrey A. Rosen, pointed toward heightened interest in technology called end-to-end encryption, which makes it nearly impossible for law enforcement and spy agencies to get access to people's digital communications.

Law enforcement and technologists have been arguing over encryption controls for more than two decades. On one side are privacy advocates and tech bosses like Apple's chief executive, Timothy D. Cook, who believe people should be able to have online communications free of snooping. On the other side are law enforcement and some lawmakers, who believe tough encryption makes it impossible to track child predators, terrorists and other criminals.

Attorney General William P. Barr, joined by his British and Australian counterparts, recently pressed Facebook's chief executive, Mark Zuckerberg, to abandon plans to embed end-to-end encryption in services like Messenger and Instagram. WhatsApp, which is owned by Facebook, already provides that tougher encryption.

"Companies should not deliberately design their systems to preclude any form of access to content even for preventing or investigating the most serious crimes," Mr. Barr wrote in a letter last month.

Here is an explanation of the technology and the stakes.

How does the encryption work?

End-to-end encryption scrambles messages in such a way that they can be deciphered only by the sender and the intended recipient. As the label implies, end-to-end encryption takes place on either end of a communication. A message is encrypted on a sender's device, sent to the recipient's device in an unreadable format, then decoded for the recipient.

There are several ways to do this, but the most popular works like this: A program on your device mathematically generates two cryptographic keys — a public key and a private key.

The public key can be shared with anyone who wants to encrypt a message to you. The private key, or secret key, decrypts messages sent to you and never leaves your device. Think of it as a locked mailbox. Anyone with a public key can put something in your box and lock it, but only you have the private key to unlock it.

How is it different from other forms of encryption?

A more common form of encryption, known as transport layer encryption, relies on a third party, like a tech company, to encrypt messages as they move across the web.

With this type of encryption, law enforcement and intelligence agencies can get access to encrypted messages by presenting technology companies with a warrant or national security letter. The sender and recipient would not have to know about it.

End-to-end encryption ensures that no one can eavesdrop on the contents of a message while it is in transit. It forces spies or snoops to go directly to the sender or recipient to read the content of the encrypted message. Or they must hack directly into the sender's or recipient's device, something that can be harder to do "at scale" and makes mass surveillance much more difficult.

Privacy activists, libertarians, security experts and human rights activists argue that end-to-end encryption steers governments away from mass surveillance and toward a more targeted, constitutional form of intelligence gathering. But intelligence and law enforcement agencies argue that end-to-end encryption makes it much harder to track terrorists, pedophiles and human traffickers.

When Mr. Zuckerberg announced in March that Facebook would move all three of its messaging services to end-to-end encryption, he acknowledged the risk it presented for "truly terrible things like child exploitation."

"Encryption is a powerful tool for privacy, but that includes the privacy of people doing bad things," he said.

Hasn't this debate been around for decades?

The debate over end-to-end encryption has had several iterations, beginning in the 1990s with the spread of Pretty Good Privacy, or PGP, software, an end-to-end encryption scheme designed by a programmer named Phil Zimmermann. As a result, the Clinton administration proposed a "Clipper Chip," a back door for law enforcement and security agencies.

But the Clipper Chip provoked a backlash from a coalition of unlikely bedfellows, including the American Civil Liberties Union; the televangelist Pat Robertson; and Senators John Kerry, the Massachusetts Democrat, and John Ashcroft, the Missouri Republican. The White House backed down in 1996.

End-to-end encryption gained more traction in 2013, after data leaked by the former National Security Agency contractor Edward J. Snowden appeared to show the extent to which the N.S.A. and other intelligence and law enforcement agencies were gaining access to users' communications through companies like Yahoo, Microsoft, Google and Facebook without their knowledge.

Encrypted messaging apps like Signal and Wicker gained in popularity, and tech giants like Apple and Facebook started wrapping user data in end-to-end encryption.

Google, which pledged to add an end-to-end encryption option for Gmail users several years ago, has not made this the default option for email. But the company does offer a video-calling app, Duo, that is end-to-end encrypted.

As more communications moved to these end-to-end encrypted services, law enforcement and intelligence services around the world started to complain about data's "going dark."

What are governments doing?

Government agencies have tried to force technology companies to roll back end-to-end encryption, or build back doors, like the Clipper Chip of the 1990s, into their encrypted products to facilitate government surveillance.

In the most aggressive of these efforts, the F.B.I. tried in 2016 to compel Apple in federal court to unlock the iPhone of one of the attackers in the 2015 mass shooting in San Bernardino, Calif.

Mr. Cook of Apple called the F.B.I.'s effort "the software equivalent of cancer." He said complying with the request would open the door to more invasive government interception down the road.

"Maybe it's an operating system for surveillance, maybe the ability for the law enforcement to turn on the camera," Mr. Cook told ABC News. "I don't know where it stops."

Privacy activists and security experts noted that any back door created for United States law enforcement agencies would inevitably become a target for foreign adversaries, cybercriminals and terrorists.

Alex Stamos, the chief security officer of Yahoo at the time, likened the creation of an encryption back door to "drilling a hole in the windshield." By trying to provide an entry point for one government, you end up cracking the structural integrity of the entire encryption shield.

The F.B.I. eventually backed down. Instead of forcing Apple to create a back door, the agency said it had paid an outside party to hack into the phone of the San Bernardino gunman.

So what now?

Governments have stepped up their calls for an encryption back door.

Last year, Australian lawmakers passed a bill requiring technology companies to provide law enforcement and security agencies with access to encrypted communications. The bill gave the government the ability to get a court order allowing it to secretly order technology companies and technologists to re-engineer software and hardware so that it can be used to spy on users.

Australia's law is based on Britain's 2016 Investigatory Powers Act, which compels British companies to hand over the keys to unscramble encrypted data to law enforcement agencies. The Australian law could apply to overseas companies like Facebook and Apple.

Australia's new law applies to network administrators, developers and other tech employees, forcing them to comply with secret government demands without notifying their employers.

Other governments are also considering new encryption laws. In India, Facebook's biggest market, officials told the country's Supreme Court in October that Indian law requires Facebook to decrypt messages and supply them to law enforcement upon request.

"They can't come into the country and say, 'We will establish a non-decryptable system,'" India's attorney general, K.K. Venugopal, told the court, referring to Facebook and other big tech platforms. India's Supreme Court has said it will reconvene on the issue in January.

1) What is the issue behind end-to-end encryption? What are the main arguments from both sides?

2) How does end-to-end encryption work? What are its specificities, and why is it so safe?

3) Why has there been a debate over encryption in the past decades? Explain the different opinions.

4) Describe the law that was passed in Australia and its implications. Are there other countries that passed or want to pass similar laws?

IV) Written expression (6 points)

Cryptography and security being the most important issues on the internet in the Big Data era, according to you, what is the best way to protect your datas ? What are the main issues behind data privacy ?

Use examples that were studied in class, or other examples that you deem relevant, and give your opinion in around 400 words.