Cryptography and privacy

Ismar Volić
Wellesley College

Amherst College
April 7, 2016

Plan of the talk

1. Privacy and technology – the current landscape
2. A brief history of cryptography
3. Public key cryptography
   (a) Diffie-Hellmann key exchange
   (b) RSA cryptosystem
   (c) Some comments on public key cryptography
4. Cryptography and current technology
5. Cryptography and politics

1. Privacy and technology – the current landscape

In recent years, consumer awareness of privacy issues has increased significantly due to several factors:

- Edward Snowden's revelations about the spying done by the National Security Agency (cell phone eavesdropping, unauthorized data access);
- Increase in usage and usefulness of "big data" and the resulting need for greater availability of information;
- Reports that apps are accessing data they do not need and sharing it (Flashlight app) or contain bugs that enable hackers access to personal information (Android);
- Privacy issues with the social media (Facebook privacy settings);
- Reports of frequent hacking and theft of personal information (Sony hack, Target theft of credit card numbers);
- Increase in (mobile) identity thefts;
- The fight between the FBI and Apple about access to the information on a San Bernardino shooter's iPhone;
- Google Street View, GPS tracking, drones, etc.

Report: NSA releases accounts of privacy violations

Published December 26, 2014 · FoxNews.com 99 309 105

(AP)

The National Security Agency has released heavily redacted accounts of its employees' violations against Americans' privacy after the Sept. 11, 2001 terror attacks.

Responding to a Freedom of Information Act lawsuit, the agency was required to file the reports with the Intelligence Oversight Board, the Wall Street Journal reports. However, the reports were released publicly Wednesday, covering

Politics Video


Kerry puts spin on US-Israel relationship


12-year-old conservative takes political world by storm

DHS cracking down on birth tourism


Kurtz: What's behind the Bibi brawl

Trending in Politics

Advice from a CMO: My Top Three Career Tips
Executive Perspectives

Don't Believe These 6 Mobile Security Myths
Consumer

How Do I Defend Against Threats in the Latest McAfee Labs Report?
Business

At Intel Security, Protecting Customers Takes Precedence
McAfee Labs

Consumer, Consumer Threat Notices

Bug Puts Nearly 750 Million Android Users at Risk of Privacy Breaches

By Gary Davis on Sep 22, 2014

About 75% of all Android devices (roughly 750 million) are at risk of falling victim to a major security vulnerability. If abused, the vulnerability could enable hackers to bypass a security mechanism called Same Origin Policy (SOP), and potentially allow them to read the contents of any open webpage and inject code to retrieve passwords, submission forms, keyboard inputs and a variety of other sensitive data. In essence: this is bad. Back in 2012, Google replaced the vulnerable browser, Android Open Source Platform (AOSP), with Chrome —

Top 10 Trending Tags

online safety
cybercrime
malware
mobile security
endpoint protection
identity theft

Socially Aware

The Law and Business of Social Media

Big Data: Big Business, Big Privacy Issues

By Susan McLean, Ann Bevitt, Karin Retzer and Reed Freeman on November 19th, 2014

Posted in Privacy

Big data is now big business.

In recent years, due to the exponential growth of databases (spurred at least in part by social media and cloud storage) and of the capability of technology to undertake data analytics on a massive scale, organisations have started to appreciate the potential hidden value that could be derived from their data.

Indeed, in March 2014, Neelie Kroes (Vice President of the EU Commission responsible for the Digital Agenda) reflected this view when she hailed a "*data gold rush… a new industrial revolution… a digital revolution fuelled by big data*".

It's certainly clear that big data analytics can drive potential significant benefits. Information produced from analytics can help companies to forecast and make better decisions, make savings and

MORRISON FOERSTER

About Socially Aware

Social media sites are transforming not only the daily lives of consumers, but also how companies interact with consumers. Here at Morrison & Foerster, across all of our practice groups, we are seeing complex, cutting-edge legal issues arising out of social media. As with the Internet boom during the mid-to-late 1990s, social media is generating new legal questions at a far faster pace than the law's ability to provide answers to such questions. In an effort to stay on top of these emerging issues, and to keep our clients and friends informed of new developments, Morrison & Foerster publishes this blog devoted to the law and business of social media.

Editors

John Delaney

Report: 10 Million Identity Theft Cases, Most Common Consumer Complaint In US

July 1, 2014 11:37 AM

Big data breaches of identity theft increased nearly 20 percent from last year and more than 10 million cases of Americans' personal records being exposed or published have already been reported in 2014 – making it the most common consumer complaint in the U.S. (Photo by Patrick Lux/Getty Images)

Related Tags: Americans' personal records, big data security breaches, Bureau of Justice Statistics, CBS News, consumer complaints, Federal Trade Commission, FTC report, health records, identity fraud, identity theft, Identity Theft Resource Center, identity thieves, Justice Department, U.S. Department of Justice

WASHINGTON (CBS DC) – Big data breaches of identity theft increased nearly 20 percent from last year and more than 10 million cases of Americans' personal records being exposed or published have already been reported in 2014 – making it the most common consumer complaint in the U.S.

OPINION

At least 80% of mobile apps have security and privacy issues that put enterprises at risk

Network World | Feb 1, 2013 3:18 PM PT

mobile malware

BYOD

mobile privacy

Mobile security

The first rule of managing a BYOD environment is to set good policies governing who can do what activities and access which data. But if you don't know what apps really do -- like harvesting a smartphone user's contact list -- you can't build effective policies. Appthority helps you manage the risk from mobile applications by analyzing what apps are actually capable of doing.

Surveys show that 3 out of 4 organizations allow BYOD (bring your own device) in the enterprise. Because of the rapid growth of the BYOD phenomenon, businesses struggle to understand their risk exposure from mobility. IT is in the uncomfortable position of playing catch-up to ensure that security isn't sacrificed in the name of employee productivity.

At first it was thought that malware posed the greatest risk to smart devices. This line of thinking was derived from our collective experience with PC operations, where malware, along with unintentional software vulnerabilities, poses one of the greatest risks to security. Malware on mobile devices is a problem, but today it doesn't even approach the magnitude of security and privacy issues that are intentionally built into well over 80% of the iOS and Android apps on the market. [See "How mobile apps can take whatever data they want from a smartphone"]

FEATURE

Smartphone apps: Is your privacy protected?

Are your apps putting your privacy at risk? We look at the dangers and solutions for Android, BlackBerry and iOS mobile platforms.

By Preston Gralla, Al Sacco and Ryan Faas

Computerworld | Jul 7, 2011 7:00 AM PT

Google Apple

Smartphone apps can do more than provide you with entertainment, information or useful services -- they can also invade your privacy.

Apps can trace your Web habits, look into your contact list, make phone calls without your knowledge, track your location, examine your files and more. They can also automatically send information such as location data to mobile ad networks.

In addition, apps can gather the phone number and the unique ID number of each type of phone: the Unique Device Identifier (UDID) on the iPhone, the International Mobile Equipment Identity (IMEI) number on the BlackBerry, and (depending on the make) the IMEI or the Mobile Equipment Identifier (MEID)

MORE LIKE THIS


Smartphone OS shootout: Android vs. iOS vs. Windows Phone

Computerworld's favorite smartphone apps

Yes, your iPhone is tracking you -- the question's why

on IDG Answers
Can cellphones get viruses?

New Facebook Messenger app raises privacy concerns

POSTED 5:49 PM, AUGUST 8, 2014, BY SHELBY BROWN, UPDATED AT 07:44PM, AUGUST 8, 2014

Heroes Among Us

Who is the hero in your life?

Click here to nominate them so Greg McQuade and CBS 6 News can share their story.

Watch CBS 6 News at 6 p.m. Thursdays for Greg's inspiring reports.

WHAT DO YOU THINK?

How late is too late to send a breaking news alert on the WTVR CBS 6 News App?

- 8 p.m.
- 9 p.m.
- 10 p.m.
- 11 p.m.
- Midnight
- I want to know about news anytime day or night.
- I don't have apps in

Apple

Apple's encryption battle with the FBI has implications well past the iPhone

As it goes to war with the Justice Department, Apple defends a core philosophy: that no one, not even its makers, should be able to look inside your phone

Sam Thielman in New York

@samthielman

Saturday 20 February 2016
07.00 GMT

The Department of Justice says that Apple is the only entity that can help them break into Syed Farook's iPhone. But would it just impact that device? Photograph: Michaela Rehle/Reuters

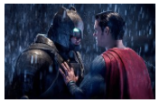
When a young married couple killed 14 people at a holiday party in San Bernardino, California, the legal implications of encryption and Apple's business model must have been the furthest thing from the minds of anyone involved.

Most popular


Hugh Jackman rescues swimmer and son from rip at Sydney's Bondi beach


Sanders crushes Clinton in Alaska and Washington Democratic caucuses


Syrian regime forces retake 'all of Palmyra' from Isis


Every single thing that is wrong with Batman v Superman: Dawn of Justice

Mark Weinstein Become a fan
Leading privacy advocate, visionary social media pioneer, and founder of MeWe.

Is Privacy Dead?

Posted: 04/24/2013 1:14 pm EDT | Updated: 06/24/2013 5:12 am EDT

While Microsoft and Google are in the latest salvo war over whose email system is truly private (calling Gmail "private" is perhaps an oxymoron), a much more significant issue is at the core: How important is our privacy? We are living in an era where Facebook's Graph Search gives strangers greater access than ever to our "private" data and Google arbitrarily steals our passwords and emails (during its Street View project). Did our forefathers misunderstand the demand for privacy as an inalienable right for law-abiding citizens in democracy? Is privacy dead? Do we care?

1. Privacy and technology – the current landscape

Privacy issues have had significant impact on consumer behavior:

- 70% of consumers say that it is important to them to know what data an app is collecting and how it is using it;
- Only 37% of consumers are comfortable sharing personal data with an app;
- 33% are *not at all* comfortable sharing personal data with an app;
- 86% of internet users are taking steps to preserve their privacy online (at least partially) and more are using VPNs like hide.me and anonymity networks like Tor;
- 50% of internet users have taken steps to hide from specific people or organizations;
- 68% if internet users do not feel that the current laws are sufficient for preserving privacy;
- 50% of internet users say they are worried about the information about them that is online (a jump from 33% in 2009);

1. Privacy and technology – the current landscape

Not only is the public outcry against privacy violations increasing, but this is also costly:

- The NSA spying revelations could cost the internet industry $180 billion in the next few years (cloud computing industry alone could lose $25-$35 billion);
- Fewer people buying problematic apps and software;
- People leaving Facebook and other social media;
- Contracts cancelled due to privacy concerns (Germany's deal with Verizon, Brazil's deal with Boeing);

1. Privacy and technology – the current landscape

As a result, tech industry is getting serious about privacy. The expectation of the protection of privacy is becoming the standard in app and software design. This is because the consumers are increasingly asking whether the maker of the product is

- concerned about the consumer's privacy,
- transparent about the data being collected, and
- careful about how the data is used.

1. Privacy and technology – the current landscape

More specifically, consumers are increasingly making sure that

- personal data protection is the default and is embedded into the product;
- the developer has a good privacy policy;
- you are notified and asked for consent any time personal data is accessed;
- it is possible to remove your personal data (in addition to uninstalling software or deleting an app);
- the product discards the data that has been collected and is no longer needed;
- the product does not use personal data for any purpose other than the one necessary for the software;

and, most important of all,

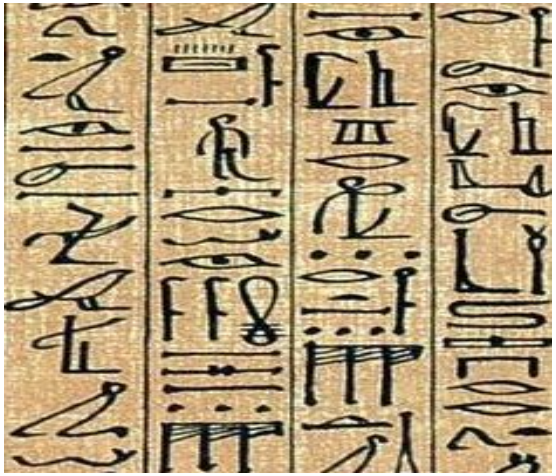
- personal information is secured with *cryptography*!!!

2. A brief history of cryptography

Cryptography is the practice and study of secure communication. The goal is to send a message so that only the intended recipient can read it. If a message is intercepted, it should be unreadable to the interceptor. Pretty much anyone who uses a computer or a smartphone uses cryptography daily – to log into websites, shop online, etc.

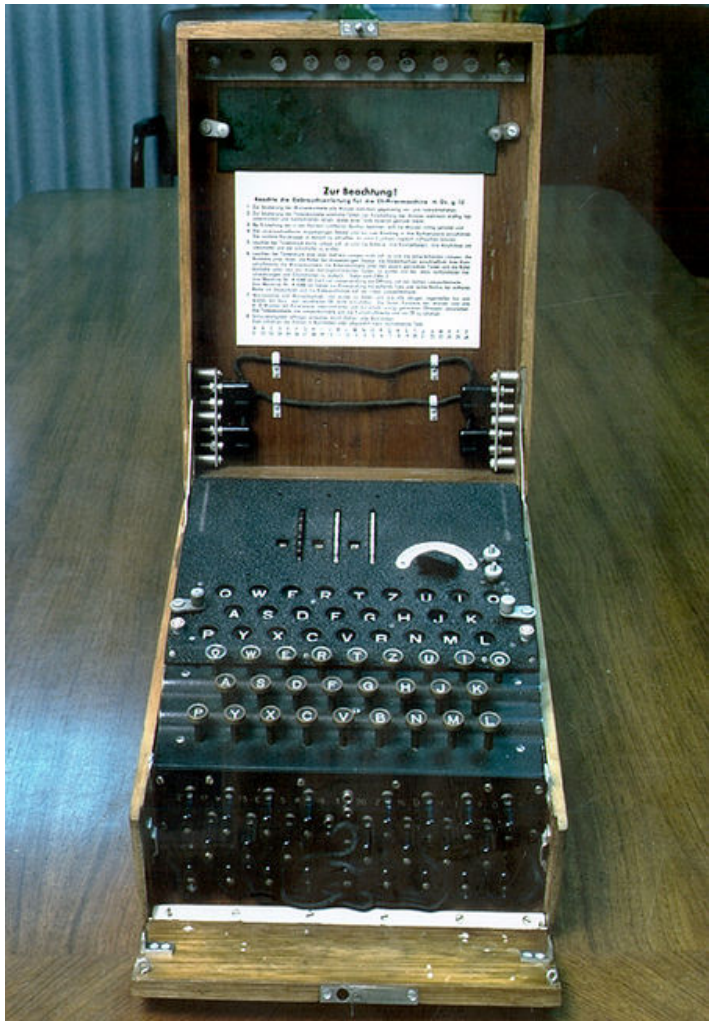
Some early examples of cryptography are

Egyptian hieroglyphics



Spartan scytale

2. A brief history of cryptography



The decryption of the German Enigma machine by the British codebreakers in World War II saved millions of lives and shortened the war by 2–4 years.

3. Public key cryptography

For most of our history, the only way to exchange information in secret was to first agree on a *keyword* and then use some kind of encryption algorithm to encrypt and decrypt messages. If the encrypted message is stolen or intercepted, it should be useless without the keyword.

With the advent of global economy in the 1960s, the exchange of keywords became impractical (there were people traveling across the world with briefcases filled with keywords to be exchanged between various institutions including banks and governments).

One of the coolest applications of mathematics is the resolution of this problem in the 1970s – two parties no longer have to meet to agree on a secret key! The exchange that leads to the establishment of a key need not even be secure – it's ok if this communication is intercepted by anyone!

In fact, entire messages can be encrypted and sent via insecure channels and only the intended recipient can read them. This is called

public key cryptography.

3(a). Diffie-Hellmann key exchange

Diffie-Hellman key exchange is the first example of public key cryptography (1976). It allows two users to agree on a key via an insecure channel. With this key, they can then encrypt communications using, say, the Advanced Encryption Standard (AES), which is built into all the computers.

First, Alice and Bob agree on a prime number p, say $p = 23$, and another number g, say $g = 5$. This is done over public channels, so everyone knows these numbers. The pair

$$(p, g) = (23, 5)$$

is called the *public key*.

In practice, p and g are hundreds of digits long (p is required to be of certain bit length, i.e. its minimum length in binary is prescribed; currently 2048-bit length is recommended).

Now we do some *modular arithmetic*.

3(a). Diffie-Hellmann key exchange

- Alice chooses a secret number a and computes

$$A \equiv g^a \pmod{p}.$$

  This means she takes the remainder upon division of g^a by p. If, say, $a = 6$, then

$$A = 8 \equiv 5^6 \pmod{23}.$$

  $a = 6$ is Alice's *private key*.

- Bob chooses a secret number b, and computes

$$B = g^b \pmod{p}.$$

  This means he takes the remainder upon division of g^b by p. If, say, $b = 15$, then

$$B = 19 \equiv 5^{15} \pmod{23}.$$

  $b = 15$ is Bob's *private key*.

(Computing A and B is not hard; there are methods for doing it fast.)

3(a). Diffie-Hellmann key exchange

- Alice sends $A = 8$ to Bob and Bob sends $B = 19$ to Alice. Everyone can see these two numbers.
- Alice takes $B = 19$ and computes

$$B^a \pmod{p} = 19^6 \pmod{23} \equiv 2$$

- Bob takes $A = 8$ and computes

$$A^b \pmod{p} = 8^{15} \pmod{23} \equiv 2$$

2 is their secret key!

The reason this works is that

$$B^a \pmod{p} = (g^b)^a \pmod{p} = (g^a)^b \pmod{p} = A^b \pmod{p}$$

3(a). Diffie-Hellmann key exchange

For an interceptor (Eve) to figure out the secret key, she would have to figure out what a or b are, and that is the same as figuring out what integer x solves one of the equations

$$A \equiv g^x \pmod{p} \quad \text{or} \quad B \equiv g^x \pmod{p}$$

In ordinary algebra, solving

$$A = g^x$$

is easy – just take logs:

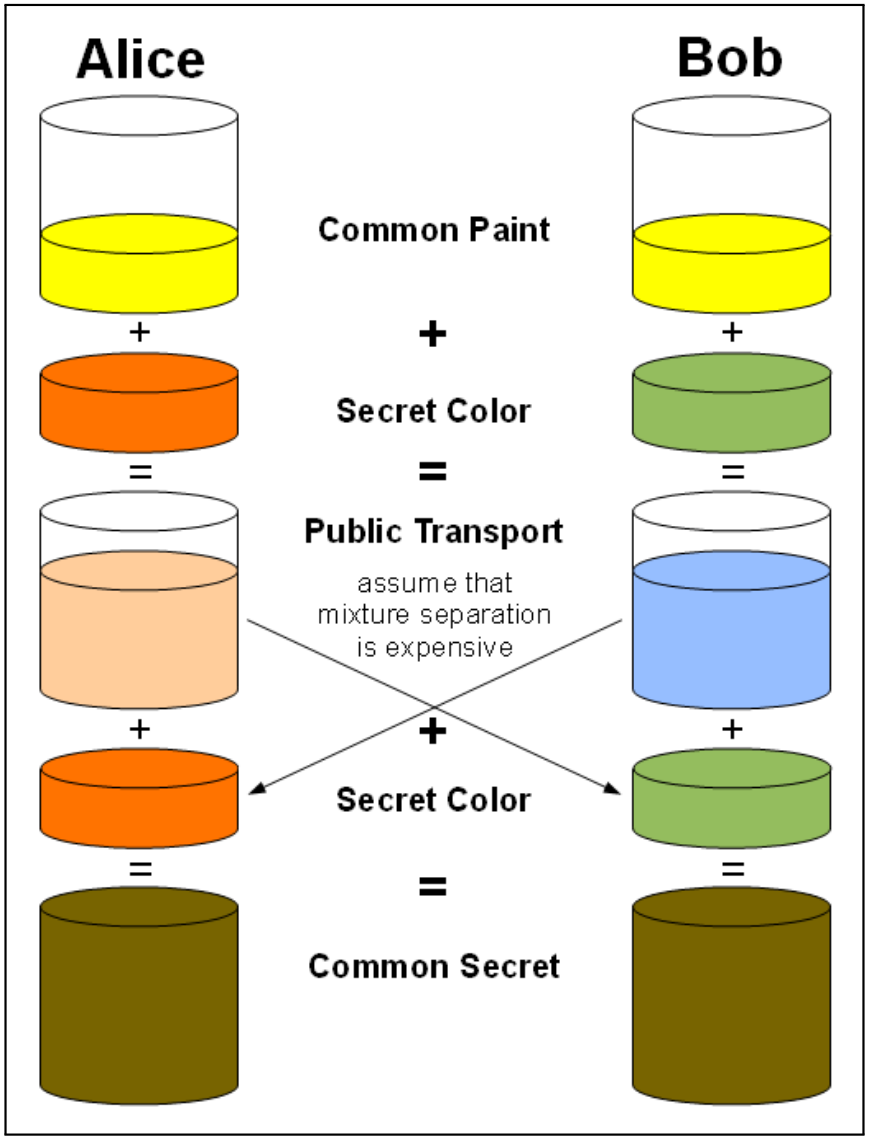
$$\ln A = x \ln g \quad \Longrightarrow \quad x = \frac{\ln A}{\ln g}.$$

But we can't do this in our modular version of the problem since this is not an integer.

The problem of solving the equation $A \equiv g^x \pmod{p}$ is called the *discrete log problem* and seems to be very hard, i.e. there is no known fast way of solving it.

This is what makes Diffie-Hellman secure!

3(a). Diffie-Hellmann key exchange



(from Wikipedia)

3(b). RSA cryptosystem

RSA (Rivest, Shamir, Adelman) was one of the first (1977) public key encryption systems that allowed the encryption of an entire message.

Suppose Alice wants to receive a secret message from Bob. She will

- Choose two large primes p and q (hundreds of digits long).
- Compute $N = pq$ and $\phi(N) = (p-1)(q-1)$.
- Choose e such that $\gcd(e, \phi(N)) = 1$ (not hard).
- Publish (e, N); this is the public *encryption key*.

Bob will take (e, N) and

- Convert his message into a string of numbers and break it up into *plaintext* blocks P of length $< N$.
- Encrypt each P by
$$C \equiv P^e \pmod{N}.$$
This is not hard to do. C is a *ciphertext* block.
- Send all ciphertext blocks C to Alice.

3(b). RSA cryptosystem

To decrypt Bob's message, Alice will

- Compute the inverse d of e modulo $\phi(N)$, i.e. find integer d such that
$$1 \equiv ed \pmod{\phi(N)}.$$
This can be done since $\gcd(e, \phi(N)) = 1$ (and can be done quickly using the Euclidean Algorithm). The number d is Alice's private key, and is called the *decryption exponent*. Thus
$$\begin{aligned} 1 \equiv de \pmod{\phi(N)} &\Leftrightarrow \phi(N) \mid ed - 1 \\ &\Leftrightarrow ed = k\phi(N) + 1, \quad \text{some integer } k. \end{aligned}$$
- Given a ciphertext block C, compute
$$C^d \pmod{N} \equiv P$$
How did this happen?
$$C^d = (P^e)^d = P^{ed} = P^{k\phi(N)+1} = (P^{\phi(N)})^k P \equiv 1^k P \pmod{N} = P.$$
The congruence in the above is by *Euler's Theorem* (from mid-18th century!). So Alice recovers the plaintext block P. She does this for all the blocks and recovers the entire message.

3(b). RSA cryptosystem

Eve wants to read Bob's message. She knows (e, N) and can intercept C. She knows C was computed by

$$C \equiv P^e \pmod{N}$$

and is trying to recover P. She needs to compute "$\sqrt[e]{C}$" (mod N). This seems to be very hard without p or q (or, equivalenty, $\phi(N)$).

She might try the *brute force attack*, namely try to factor $N = pq$ by checking whether various primes divide N. Suppose N is 100 digits long. Then

$$N \approx 10^{100}$$

and Eve needs to check whether any of the primes from 2 to $\sqrt{10^{100}} = 10^{50}$ are factors of N. By *Prime Number Theorem*, there are about

$$\frac{10^{50}}{\ln(10^{50})} \approx 10^{48}$$

primes in that range.

3(b). RSA cryptosystem

So Eve expects that she might need to perform up to 10^{48} divisions of N by prime numbers.

But nobody even has the list of the first 10^{48} primes!!! It takes about 14 bytes to store a 48-digit number, so to store such a list would take about

$$14 \times 10^{48} \text{ bytes } = 14 \times 10^{36} \text{ terabytes.}$$

So it would take 14×10^{36} computers with 1TB drives to just *store* all those primes!

There are better ways to try to crack RSA, but none of them are fast. This is what makes RSA secure!

3(c). Some comments on public key cryptography

Some more sophisticated cryptosystems are

- *Elliptic curve cryptosystems* – use the fact that the solutions to the equation $y^2 = x^3 + ax + b$ form a group and that solving the *elliptic curve discrete log problem* is hard.
- *Lattice-based cryptosystems* – use the fact that finding a *shortest vector* in a lattice is hard.
- *Quantum cryptosystems* – use the fact that observing a message changes it, so Alice and Bob know when someone is watching. (This is still not fully functional.)

The security of all the known cryptosystems relies on the existence of a *one-way function* that is easy to compute (like modular exponentiation or multiplication of primes) but whose inverse seems to be hard to compute. So the security of the most important cryptosystems relies on the *practical irreversibility* of some process.

Open problem: Is there a function whose inverse is *provably difficult*, i.e. a function whose inverse *cannot be easy*?

4. Cryptography and current technology

Public key cryptosystems are used for

- *Encryption* – protect data from intruders or share it with the intended audience;
- *Authentication* – determine whether someone or something is what it claims to be;
- *Verification* – determine whether the data was sent by a known sender and that it was not modified in transit.

Some basic protocols that use public key cryptography are

- *Transport Layer Security* (TLS) for encrypting data in transit ("`https://`");
- *GNU Privacy Guard* (GPG) for encrypting and signing data;
- *Pretty Good Privacy* (PGP) for encrypting texts, emails, and other communications.

You should make sure websites that handle sensitive information use TLS and use GPG/PGP for encryption of your personal data (software is free for download).

4. Cryptography and current technology

If used properly, cryptography is a full-proof way to secure data. As a response to the public's concerns over privacy and increased use of tools like GPG and PGP, cryptography is coming to the forefront of the discussion. Companies and developers are taking various measures:

- Apple's iOS8 encrypts all the data on the iPhone (so not even Apple can access it);
- More developers are adding encryption measures to their products, including TLS and GPG;
- Email providers are adding easier encryption of emails, usually with PGP (Chrome extension);
- More apps and software are produced just for encrypting other data on the computer or a smartphone.

It is thus becoming easier to protect our privacy and we should all take advantage of this. Understanding how encryption works (i.e. understanding the math behind it) gives you additional facility to make informed decisions and even be a part of the discussion about privacy.

However, there is something to keep in mind...

4. Cryptography and politics

Governments do not like cryptography!

Cryptography allows criminals to communicate securely, and law enforcement agencies would like to be able to intercept and decrypt their messages (intercepting is easy). Most countries have a spy agency that does this.

U.S. National Security Agency

5. Cryptography and politics

German Bundesnachrichtendienst

5. Cryptography and politics

Echelon Global Surveillance System
(United Kingdom, Australia, Canada, New Zaeland, U.S.)

5. Cryptography and politics

Bosnian Intelligence and Security Agency

5. Cryptography and politics

U.S. government has attempted to regulate cryptography and build *backdoors*, i.e. put in insecurities into cryptosystems that would allow it, but nobody else, to decrypt communications.

The most famous instances of this occurred during the *First Crypto War* of the 1990s where the U.S. goverment tried to

- Add the *Clipper chip*, which implemented encryption with a backdoor, into mobile phones;
- Weaken the *Data Encryption Standard*, the encryption system built into all the computers at the time;
- Prosecute the creator of PGP for publishing it on the internet.

All three attempts failed, and the first crypto wars were thought to be over. However, Snowden's revelations show that they might not be.

5. Cryptography and politics

The files released by Snowden show that there is still a secret war being waged in the cryptography arena. They show that the NSA has

- Since 2000 invested billions of dollars into preserving its ability to eavesdrop (focusing on encryption in TLS and VPNs, and looking for ways of looking into protected content of Google, Yahoo, Facebook, Hotmail, and other companies);
- Put in backdoors into elliptic curve-based random number generator that weakens encryption systems used by millions of people;
- Hacked (along with its British counterpart) into the internal network of the world's largest manufacturer of SIM cards, Gemalto, and stole the encryption keys that protect the privacy of cell phone communications across the world;
- Been working with internet companies to build backdoors into their products ($250-million Sigint Enabling Project);
- Been lobbying for legislature that weakens encryption standards, etc.

But the NSA is not alone; government regulation of cryptography occurs globally:

5. Cryptography and politics

Cryptography is treated as a *dual-use technology*, namely it has commercial and military value (i.e. it can be thought of as a weapon). With the *Wassenaar Arrangement* of 1994, over 40 countries now put limitations on import and export of cryptography and products using cryptography. These limitations are largery dictated by the U.S. government and the NSA.

For example, if you try to submit an app to Apple or Windows, you see something like

> *The Bureau of Industry and Security in the United States Department of Commerce regulates the export of technology that uses certain types of encryption. All apps must go through the encryption review. They are uploaded to a server in the United States, which means that your product is exported from the United States and is captured by U.S. export laws. This requirement applies even if you plan to distribute apps only within your own country. Failure to comply could result in severe penalties.*

Summary

In conclusion, as a technology-savvy citizen of the world, you should

- Be aware of the global increase in concern over privacy;
- Make sure the product you are using respects privacy and handles private data carefully;
- You should use (and understand) cryptography!

Thank you!