CISC 468: CRYPTOGRAPHY

LESSON 1: INTRODUCTION

Furkan Alaca

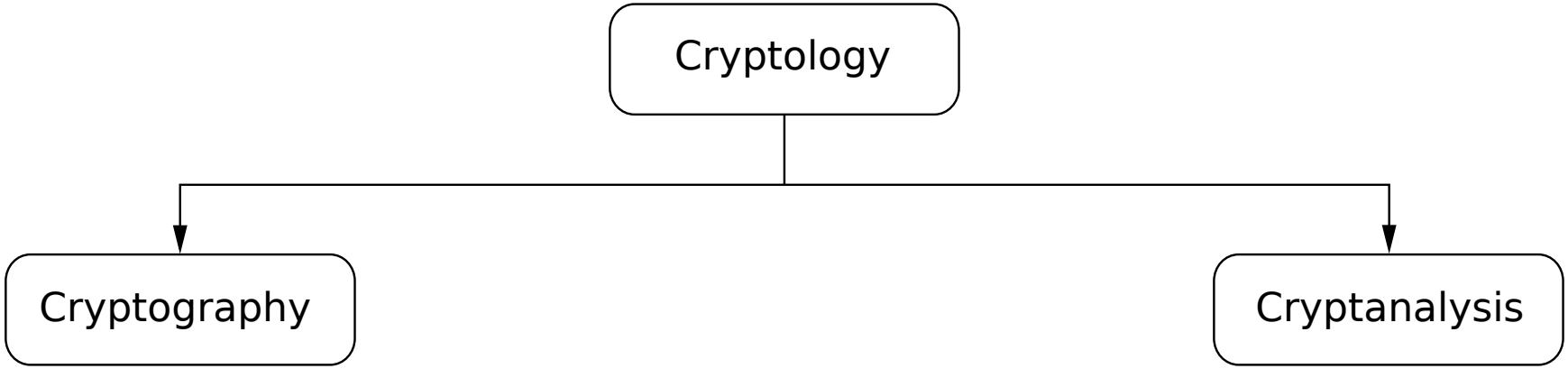
TODAY, WE WILL LEARN ABOUT...

1. Objectives and history of the field of cryptography
2. How cryptography relates to information security
3. The structure and learning objectives of this course

READINGS

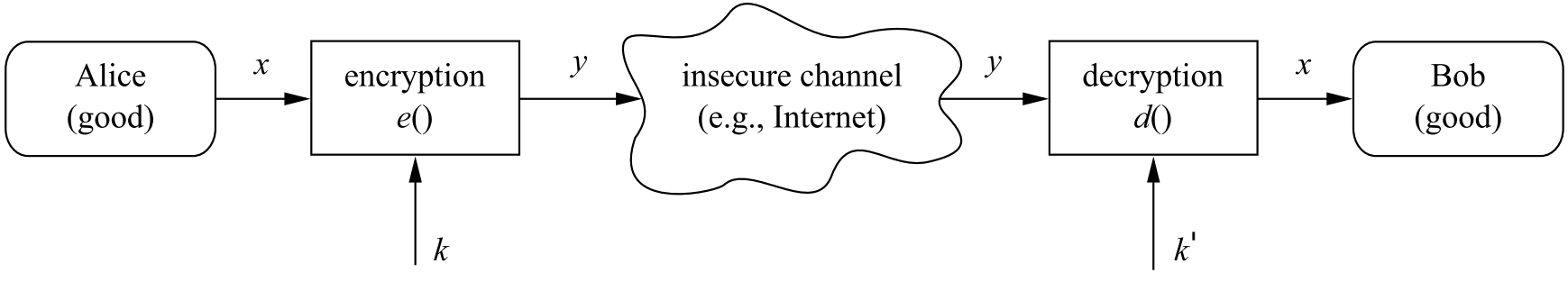
- Ch. 1.1 (Overview of Cryptology), Paar & Pelzl
- Ch. 1.1 (Fundamental goals of computer security), Van Oorschot

WHAT IS CRYPTOGRAPHY?

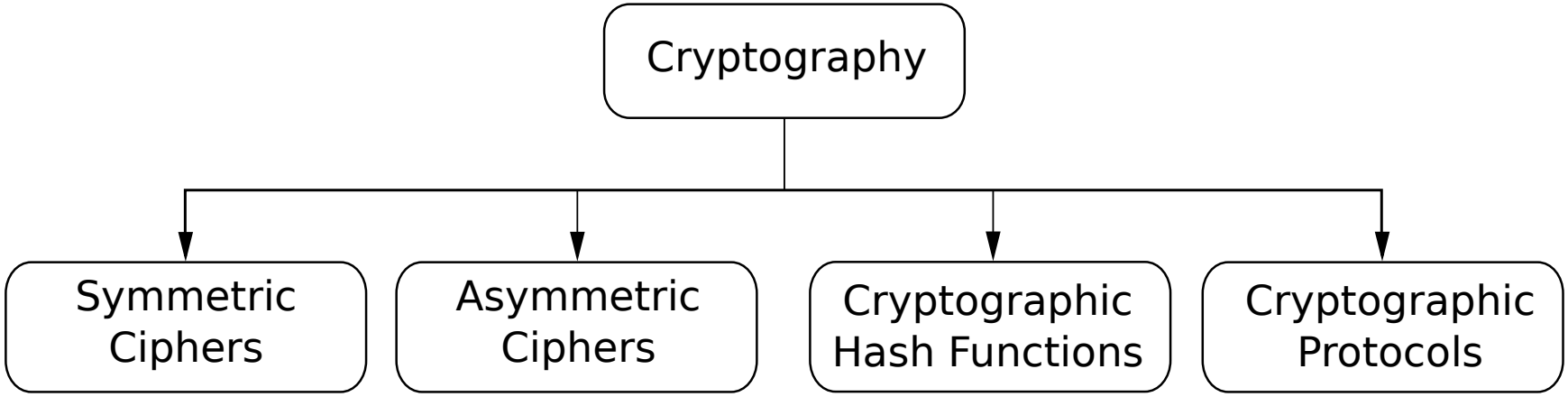


Source: Paar & Pezl, Fig. 1.3

ENCRYPTION AND DECRYPTION: A GENERIC MODEL

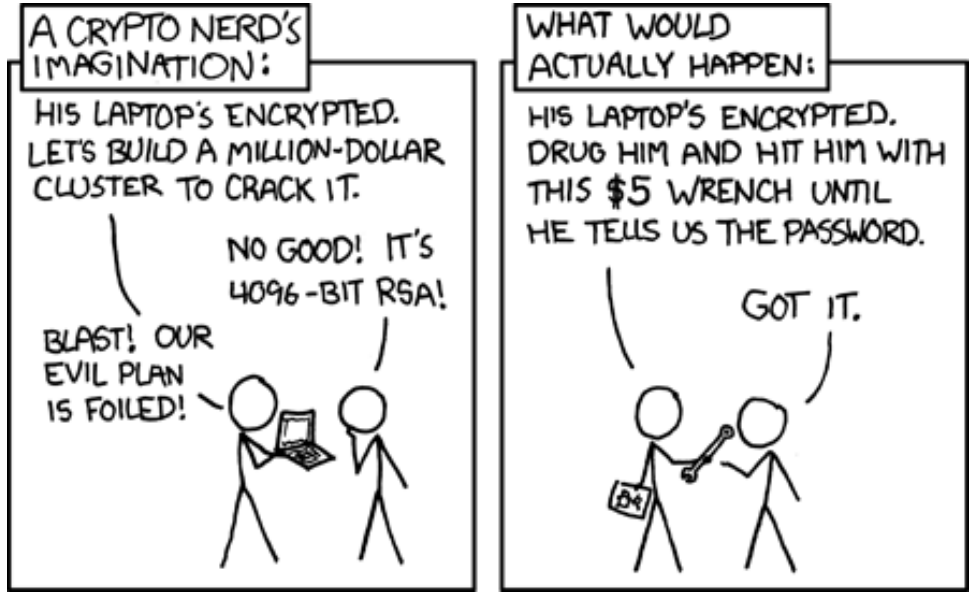


MAIN BRANCHES OF CRYPTOGRAPHY



ATTACKS ON ENCRYPTION

- Classical cryptanalysis: Find an efficient way to reverse the algorithm without knowledge of the key
- Brute-force: Try all possible keys
- Side-channel attacks: Infer knowledge of the key or plaintext by taking physical measurements
  - e.g., computation time, power consumption
- Social engineering: Trick or coerce the legitimate party into revealing the key or plaintext


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

Source: xkcd

WHAT IS INFORMATION SECURITY?

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Source: NIST Glossary of Key Information Security Terms

WHAT IS INFORMATION SECURITY? (2)

The combined art, science, and engineering practice of protecting computer-related assets from unauthorized actions and their consequences, either by preventing such actions or detecting and then recovering from them.

Source: Van Oorschot (Ch. 1)

SECURITY GOAL (1): *CONFIDENTIALITY*

- Assure that confidential information is not disclosed to unauthorized parties.
  - Stored data
  - Data in transit (transmitted over network)
- *Cryptography* is a technical means of protecting confidentiality
  - There are also other technical means, such as *Access Control*

SECURITY GOAL (2): *INTEGRITY*

- *Data integrity:* Assure that information and programs are changed only in a specified and authorized manner
- *System integrity:* Assure that a system functions as intended, free from any unauthorized manipulation
- *Cryptography* is also a technical means of protecting integrity
  - Again, there are other technical means, such as *Access Control*

Windows patches can be intercepted and injected with malware

Researchers say Windows machines that fetch updates from an enterprise update server not configured to use encryption are vulnerable to an injection attack.

By Zack Whittaker for Zero Day | August 6, 2015 -- 17:45 GMT (10:45 PDT) | Topic: Security

Can you be certain that patches served through Windows Update aren't laced with malware?

Researchers at UK-based security firm Context demonstrated at the Black Hat conference in Las Vegas on Wednesday how hackers can compromise corporate networks by exploiting a weakness in Windows' update mechanism.

KNOB —

New Attack exploiting serious Bluetooth weakness can intercept sensitive data

"KNOB" forces devices to use encryption keys that are trivial to break.

DAN GOODIN - 8/17/2019, 9:56 AM

Researchers have demonstrated a serious weakness in the Bluetooth wireless standard that could allow hackers to intercept keystrokes, address books, and other sensitive data sent from billions of devices.

Dubbed Key Negotiation of Bluetooth—or KNOB for short—the attack forces two or more devices to choose an encryption key just a single byte in length before establishing a Bluetooth connection. Attackers within radio range can then use commodity hardware to quickly crack the key. From there, attackers can use the cracked key to decrypt data passing between the devices. The types of data susceptible could include keystrokes passing between a wireless keyboard and computer, address books uploaded from a phone to a car dashboard, or photographs exchanged between phones.

SECURITY GOAL (3): *AVAILABILITY*

- Assure timely and reliable access to services by authorized users
- Protect from *Denial of Service* attacks aiming to delete/disrupt or overwhelm resources

PRACTICE QUESTIONS

Identify the computer security goal(s) violated by the following real-world examples.

NOT THIS AGAIN —

Xbox Live pummeled by DDoS attack; hacker group claims responsibility

Phantom Squad had threatened to mimic Lizard Squad, take down gaming services.

MARK WALTON - 12/18/2015, 8:35 AM

In an attack aping the work of the infamous Lizard Squad hacking group, the similarly titled Phantom Squad has claimed responsibility for a DDoS attack on Microsoft's Xbox Live service. While the service is now currently back up, some users experienced problems logging in overnight. Sony's PlayStation Network was not affected.

The attacks follow threats issued by Phantom Squad on its now suspended Twitter account. The group threatened to take down both Xbox Live and PlayStation Network over the Christmas period for as long as a week. Responding to criticism over the threats, the group said: "Why do we take down PSN and Xbox Live? Because cyber security does not exist," and "Some men just want to watch PSN and Xbox Live burn."

This was followed by a tweet yesterday reading "Xbox Live #Offline," coinciding with the reported Xbox Live problems. "Maybe if you guys didn't talk shit about us, we would not hit Xbox Live this early," read another tweet. The group then threatened to take down PlayStation Network next, before its Twitter account was taken offline.

BIZ & IT —

Potent LastPass exploit underscores the dark side of password managers

Developers are scrambling to fix flaw that allows theft, malicious code execution.

DAN GOODIN - 3/28/2017, 3:06 PM

Developers of the widely used LastPass password manager are scrambling to fix a serious vulnerability that makes it possible for malicious websites to steal user passcodes and in some cases execute malicious code on computers running the program.

The flaw, which affects the latest version of the LastPass browser extension, was briefly described on Saturday by Tavis Ormandy, a researcher with Google's Project Zero vulnerability reporting team. When people have the LastPass binary running, the vulnerability allows malicious websites to execute code of their choice. Even when the binary isn't present, the flaw can be exploited in a way that lets malicious sites steal passwords from the protected LastPass vault. Ormandy said he developed a proof-of-concept exploit and sent it to LastPass officials. Developers now have three months to patch the hole before Project Zero discloses technical details.

"It will take a long time to fix this properly," Ormandy said. "It's a major architectural problem. They have 90 days, no need to scramble!"

Montreal

Personal data of 2.7 million people leaked from Desjardins

Data breach affects more than 40% of Quebec-based credit union's clients and members

Jonathan Montpetit · CBC News · Posted: Jun 20, 2019 2:29 PM ET | Last Updated: June 20

An employee with "ill-intention" at Desjardins Group collected information about nearly three million people and businesses and shared it with others outside the Quebec-based financial institution, officials revealed Thursday.

The data breach affects around 2.7 million people and 173,000 businesses, more than 40 per cent of the co-operative's clients and members. Desjardins is the largest federation of credit unions in North America, with outlets across Quebec and Ontario.

The leaked information includes names, addresses, birth dates, social insurance numbers, email addresses and information about transaction habits.

MORE INFORMATION SECURITY GOALS

- *Authorization:* Access to resources limited to authorized parties
- *Authentication:* Determine that a principal (e.g., user, server, hardware device, mobile app) is genuine, i.e., that it is in fact what it claims/appears to be
- *Accountability:* Identify principals responsible for past actions
- Discussion: Explain at a high level how onQ enforces authentication, authorization, and accountability.

AFTER TAKING THIS COURSE, YOU SHOULD BE ABLE TO...

1. Describe underlying mathematical concepts and properties of modern cryptographic algorithms and describe their limitations.
2. Critically evaluate the use of cryptographic algorithms in real-world computer protocols and systems to determine security objectives achieved.
3. Achieve specific security goals by appropriately applying/utilizing cryptographic algorithms.
4. Demonstrate practical attacks to break vulnerable applications of cryptographic algorithms.

COURSE EVALUATION SCHEME

- Three quizzes, 12.5% each
- Three assignments, 12.5% each
- Final project, 25%

ACADEMIC INTEGRITY

The work you submit must be your own, done without participation by others. It is an academic offence to hand in anything written by someone else without acknowledgement.

ACADEMIC INTEGRITY DON'TS:

- Looking at another student's assignment
- Using code that you haven't written, without attribution
- Asking someone else (e.g., classmate or stranger on Stack Overflow) to write your code
- You are not helping your friend when you give them a copy of your assignment
- You are hurting your friend when you ask them to give you a copy of their assignment

DO HELP EACH OTHER BY:

- Explaining and/or clarifying concepts
- Solving practice questions together (e.g., from the textbook)
- Helping each other understand documentation, error messages

> *Give a man a fish and feed him for a day. Teach a man to fish and you feed him for a lifetime.*

HOW TO GET SUPPORT

- Use the Discussion Board
  - Ask questions about course content here (not by e-mail), so all students can benefit
  - Instead of asking "How do I do the assignment?", ask questions to understand tools/concepts needed for completing the assignment, common mistakes, debugging techniques, etc.
- Office Hours
- Microsoft Teams