Cryptography Course Introduction

Dr Basel Halak

Security Threats

UNIVERSITY OF Southampton
School of Electronics and Computer Science

Man Hacks Monitor, Screams at Baby Girl

by KEITH WAGSTAFF

Welcome to the Internet of things. Creepy things.

Last week, Fox 19 reported that a man hacked into an Internet-enabled baby monitor in a home in Cincinnati, Ohio, and started screaming "Wake up baby!" at a 10-month-old girl.

Source: http://www.nbcnews.com/tech/security/man-hacks-monitor-screams-baby-girl-n91546

UNIVERSITY OF Southampton
School of Electronics and Computer Science

Security Threats

Broken Hearts

Source: https://en.wikipedia.org/wiki/Broken_Hearts_(Homeland)

UNIVERSITY OF Southampton
School of Electronics and Computer Science

Security Threats

- **Black Hat USA 2015: The full story of how that Jeep was hacked**

Black Hat USA 2015: The full story of how that Jeep was hacked

August 6, 2015 Alex Drozhzhin Featured Post, News, Security, Threats

Recently we wrote about the now-famous hack of a Jeep Cherokee. At Black Hat USA 2015, a large security conference, researchers Charlie Miller and Chris Valasek finally explained in detail, how exactly that hack happened.

At the start of their research Miller and Valasek tried to hack the multimedia system of Jeep through Wi-Fi connection — Chrysler, the manufacturer of the vehicle, offers this option by subscription. It turned out, that it isn't that hard to hack this Wi-Fi due to the fact that the Wi-Fi password is generated automatically, based on the time when the car and it's multimedia system — the head unit — is turned on for the very first time.

Source: https://blog.kaspersky.com/blackhat-jeep-cherokee-hack-explained/9493/

Applications

UNIVERSITY OF Southampton
School of Electronics and Computer Science

WAR

Banking

Internet of Things

Secure Communication

Smart Card

GSM

Content Protection

HTTPS

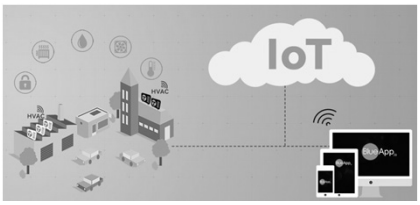
WAP2

DVDs and Blu-Ray disks

UNIVERSITY OF Southampton
School of Electronics and Computer Science

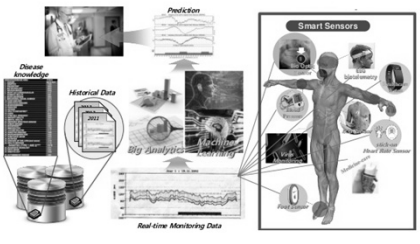
Security of IoT is a major concern

Smart Lighting



Heating, Ventilating, And Air Conditioning

Smart Homes



Smart Health

Smart Cars

Ongoing Dilemma: Privacy vs. Security

- UK PM wanted to ban encryption in 2015

http://www.bbc.co.uk/news/technology-30794953

What is Cryptography

- **Cryptography** the science of secret writing with goal of hiding the meaning of the message.
- It provide the basic building blocks to construct secure systems
- **However**, it does not provide solutions to all security problems. It is only reliable if implemented properly
- **Cryptanalysis – analyzing (breaking) secrets**

  Cryptanalysis is what attacker does

  Decipher or Decryption is what legitimate receiver does.

House Keeping Rules

- **Learning Resources and Lecture Slides:**

https://secure.ecs.soton.ac.uk/notes/elec6242/

- **Mobile Phone are not allowed**
- **Eating and drinking is not allowed**
- **Avoid late arrival**

Essential Background Knowledge

- **Make sure you are comfortable with the type of mathematical material that is planned, specifically:**

1. Discrete Probability Theory
2. Computational number theory and Algebra

What is Cryptography

Quiz: Decrypt the following message

oiit gepq erh gevvc sr

What is Cryptography

Quiz: Decrypt the following message

oiit gepq erh gevvc sr

the

ABCDEFGHIJKLMNOPQRSTUVWXYZ

T

PQRST

PQRSTUVWXYZ

PQRSTUVWXYZABCDEFGHIJKLMNO

What is Cryptography

Quiz: Decrypt the following message

oiit gepq erh gevvc sr

t

ABCDEFGHIJKLMNOPQRSTUVWXYZ
PQRSTUVWXYZABCDEFGHIJKLMNO

What is Cryptography

Quiz: Decrypt the following message

oiit gepq erh gevvc sr

dxxi vtef tgw vtkkr hg

ABCDEFGHIJKLMNOPQRSTUVWXYZ
PQRSTUVWXYZABCDEFGHIJKLMNO

What is Cryptography

Quiz: Decrypt the following message

oiit gepq erh gevvc sr

and

ABCDEFGHIJKLMNOPQRSTUVWXYZ

A

ABCDEFGHIJKLMNOPQRSTUV

WXYZABCDEFGHIJKLMNOPQRSTUV

What is Cryptography

Quiz: Decrypt the following message

oiit gepq erh gevvc sr

and

ABCDEFGHIJKLMNOPQRSTUVWXYZ

WXYZABCDEFGHIJKLMNOPQRSTUV

What is Cryptography

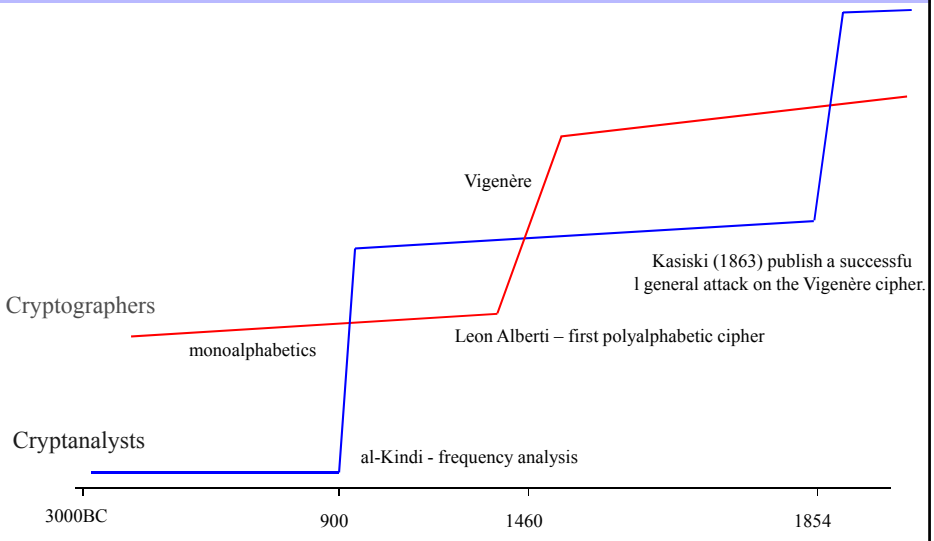
Quiz: Decrypt the following message

oiit gepq erh gevvc sr

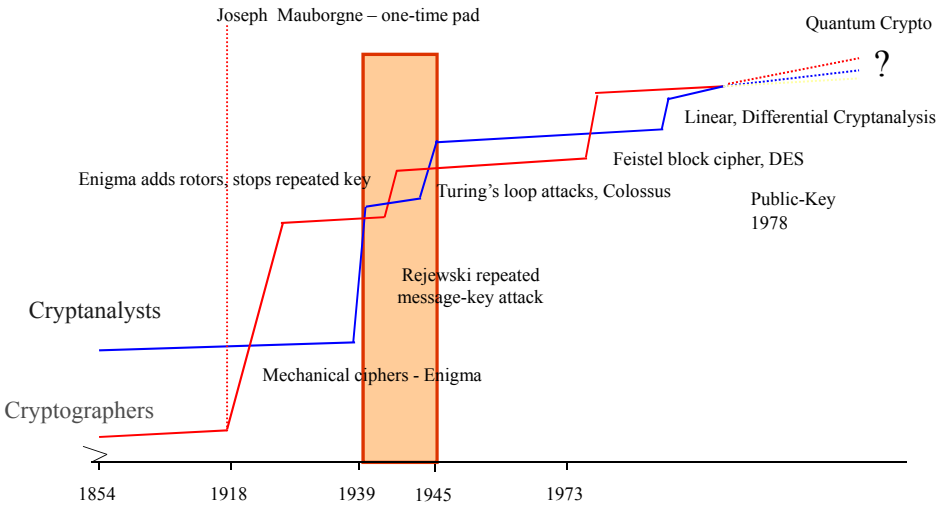
keep calm and carry on

ABCDEFGHIJKLMNOPQRSTUVWXYZ
WXYZABCDEFGHIJKLMNOPQRSTUV

Cryptography : A Brief History (First 4000 years)



Cryptography : A Brief History (last 120 years)



Cryptography : A Brief History (October 2015)

- **Toshiba and BT boast 'unhackable' network security with new quantum cryptography tech**

http://www.computing.co.uk/ctg/news/2428904/toshiba-and-bt-boast-unhackable-network-security-with-new-quantum-cryptography-tech

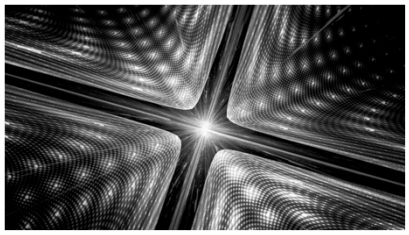
Cryptography : A Brief History (January 2016)

'Unbreakable' quantum crypto might not be as secure as first thought...

http://www.computing.co.uk/ctg/news/2440916/unbreakable-quantum-crypto-might-not-be-as-secure-as-first-thought

Cryptography : A Brief History(DEC 2016)

- US Government Escalates Push for Post-Quantum Cryptography (https://www.meritalk.com/articles/cryptographers-rally-to-nist-call-for-quantum-computer-algorithms/)



NIST announced a call for proposals for post-quantum cryptography standardization on Dec. 20. One or more of the proposed algorithms will ultimately replace some of NIST's cryptographic standards that are most vulnerable to quantum computer

Learning Outcomes

- **At the end of this course you should be able to:**

1. Describe the historical struggles between code makers and code breakers.
2. Explain the working principles of cryptographic primitives using appropriate mathematics.
3. Reason about the security of cryptographic primitives.
4. Perform cryptanalysis on relatively simple ciphers.

Course Structure

The aim of this course is to outline the mathematical principles and algorithms which underpin cryptographic primitives . Below is a list of topics which will be covered:

- Classic Ciphers
- Symmetric Key Cryptosystems (3DES, AES..)
- Public Key Cryptosystems
- Message Authentication Codes
- Modular Arithmetic and Group theory
- Quantum Cryptography
- Post Quantum-Computing Cryptosystems

Assessments

Assessment Type	Date	Contribution
Cryptanalysis Coursework	March 7th	20%
Exam	TBA	80%

Cryptanalysis Assignment

- **It is going to be an individual assignment**
- **It consists of a number of challenges which are unique for each students**
- **Examples from last years includes:**

1. Classic cipher cryptanalysis
2. Construction of example encryption systems

Exam

- **The course has changed over the years so not all past exam questions are relevant (e.g. Huffman Codes).**
- **This year, you will need to answer THREE out of FOUR possible questions.**

Essential Background Knowledge

- **Make sure you are comfortable with the type of mathematical material that is planned, specifically:**

1. Discrete Probability Theory

http://en.wikibooks.org/wiki/High_School_Mathematics_Extensions/Discrete_Probability

2. Computational number theory and Algebra

http://shoup.net/ntb/ntb-v2.pdf

Quiz

Quiz: Decrypt the following message:

Il uva hmyhpk vm nyvdpun zsvdsf, il hmyhpk vusf vm zahukpun zapss