Cryptography Principles

Yu Zhang

Harbin Institute of Technology

Cryptography, Autumn, 2016

What cryptography is and is not

Cryptography is:

- A tremendous tool
- The basis for many security mechanisms
- Secure communication:
 - web traffic: HTTPS (SSL/TLS)
 - wireless traffic: 802.11i WPA2 (and WEP), GSM, Bluetooth
 - encrypting files on disk: EFS, TrueCrypt
 - content protection: DVD (CSS), Blu-ray (AACS)
 - user authentication

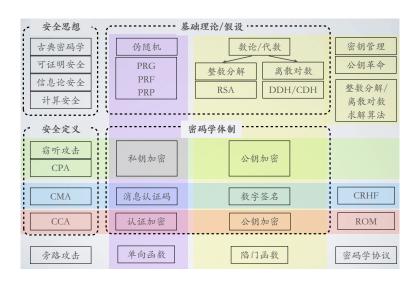
Cryptography is **NOT**:

- The solution to all security problems
- Reliable unless implemented and used properly
- Something you should try to invent yourself

Outline

- Classic cryptography, Perfect Secrets
- Private Key Encryption, MAC, Block Cipher, OWF
- Number Theory, Factoring and Discrete Log
- Key Management, Public Key, Digital Signature
- TPD, Random Oracle Model
- Cryptographic Protocols (Many magics here)

Syllabus [in Chinese]



We will learn from Turing Award recipients

- 1995 M. Blum
- 2000 A. Yao
- 2002 R. Rivest, A. Shamir, L. Adleman
- 2012 S. Micali, S. Goldwasser
- 2013 L. Lamport
- 2015 M. E. Hellman, W. Diffie

Purposes

- Learn what the rigorous information security is
- Learn how to secure information rigorously
- Learn how mathematics interplays with engineering

Textbooks, Slides, & Contact

Textbook: Introduction to Modern Cryptography, Jonathan

Katz and Yehuda Lindell, Chapman & Hall/CRC.

MOOC: Stanford Dan Boneh's Cryptography @Coursera

Slides: https://github.com/YuZhang/crypto2014

Office: 710 Zong-He-Lou

Email: yuzhang AT hit.edu.cn

Grades

■ Composition:

Homework: $4 \times 5 = 20\%$ (Homework $1 \sim 5$)

Final Exam: 80%

Extra: 5% for outstanding homework (Homework $1 \sim 6$)

- How to score high:
 - Read the textbook IMC
 - Do homework by yourself
 - No Plagiarism! Otherwise, -10 point penalty each time.

One more thing, we will read comics [xkcd:177]

I'M SURE YOU'VE HEARD ALL ABOUT THIS SORDID AFFAIR IN THOSE GOSSIPY CRYPTOGRAPHIC PROTOCOL SPECS WITH THOSE BUSYBODIES SCHNEIER AND RIVEST, ALWAYS TAKING ALICE'S SIDE, ALWAYS LABELING ME THE ATTACKER.



YES, IT'S TRUE. I BROKE BOB'S PRIVATE KEY AND EXTRACTED THE TEXT OF HER MESSAGES. BUT DOES ANYONE REALIZE HOW MUCH IT HURT?



HE SAID IT WAS NOTHING, BUT EVERYTHING FROM THE PUBLIC-KEY AUTHENTICATED SIGNATURES ON THE FILES TO THE LIPSTICK HEART SWEARED ON THE DISK SCREAMED "ALICE."



I OIDN'T WANT TO BELIEVE
OF COURSE ON SOME LEVEL
I REALIZED ITWE A KNOWNPAINTEXT ATTACK. BUT I
COULDN'T ADMIT IT UNTIL.
I SAW FOR MYSELF.



SO BEFORE YOU SO QUICKLY UBBEL
ME A THIRD PARTY TO THE COMMUNICATION, JUST REMEMBER:
I LOVED HIM FIRST. WE
HAD SOMETH ING AND SHE
/ TORE IT AWAY. SHE'S
THE ATTACKER, NOT ME.