601.445/600.645
Practical Cryptographic Systems

Introduction

Instructor: Matthew Green, Spring 2024

Intro

- What is a Cryptographic System?
  - A security system
  - Uses cryptography
- Many fascinating ways to get it wrong!
  - “Practical”:
    People actually use it & depend on it

How many systems can that be?


DVD-Cracking Teen Acquitted
Associated Press 01.07.03
Bluetooth
Cell phone, VoIP technologies lack security, experts say
2015-12 Out of Cycle Security Bulletin: ScreenOS: Multiple Security issues with ScreenOS (CVE-2015-7755, CVE-2015-7756)
[JSA10713] Show KB Properties
PRODUCT AFFECTED:
Please see below for details.
Blu-ray Disc
New attack cracks WEP in record
The fact that 104-bit WEP has been c
is in itself not ne
speed with whic
attack works is.
The DROWN Attack
DROWN check
Paper
Q&A
DROWN is a serious vulnerability that affects HTTPS and other services that rely on SSL and TLS, some of the essential cryptographic protocols for Internet security. These protocols allow everyone on the Internet to browse the web, use email, shop online, and send instant messages without third-parties being able to read the communication.
DROWN allows attackers to break the encryption and read or steal sensitive
Rese
hers claim GSM calls can be ha
on the chea
t Cards
SSH.
penSSH
EEPING YOUR COMMUNIQUÉS SECRET

This course

- Not a course in theoretical cryptography
  - We'll cover cryptography from a practical angle, aim is to apply cryptography
- Practice-oriented tutorial
  - examine how systems fail
  - how we can design against it
  - what can't we design against
- Driven by your questions & the news

What you'll come away with

- A grounding in cryptographic techniques
  - The right algorithms
  - Strengths & weaknesses, applicability
  - A feel for the design/evaluation process
  - Introduction to standards (e.g., FIPS)
  - Enough to know where to look for more
- Knowledge of our own limitations
  - Building secure systems is hard
    (even for experts)

Grading, Text

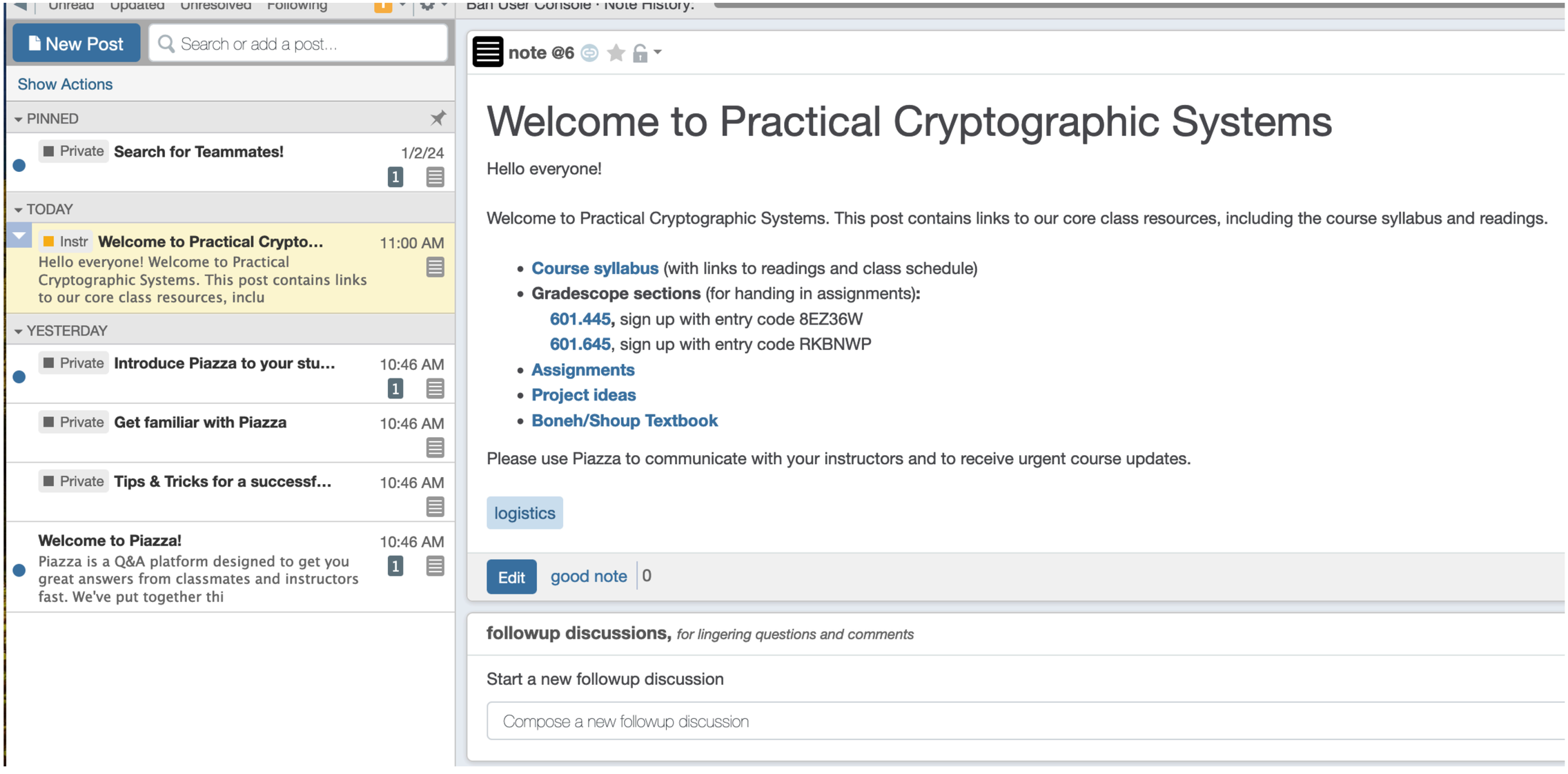
- Grading Policy:
  - 30% Exams (Midterm)
  - 35% Programming Assignments,
  - 10% Written Assignments
  - 15% Project
  - 10% Class participation
- Main text:
  - Boneh/Shoup: Graduate Course in Applied Cryptography

Piazza

- We will use Piazza for all communications, including schedule changes and snow days
- You must sign up!
- You can also find links to all of the class resources (syllabus, readings, Gradescope, etc.)

https://piazza.com/class/lqwivnfma0526

Syllabus and Resources



https://github.com/matthewdgreen/practicalcrypto2024

Syllabus

matthewdgreen edited this page 6 minutes ago · 3 revisions

Dates are subject to radical & arbitrary change. Reading assignments are due prior to beginning of the subsequent class.

Textbooks and Resources:

- Dan Boneh, Victor Shoup: **A Graduate Course in Applied Cryptography v0.6** (PDF available online)
- Ross Anderson: **Security Engineering** (PDFs available online)
- *Optional Reference:* Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone: Handbook of Applied Cryptography (PDFs available online)
- Class Piazza:
- Turn in assignments via Gradescope
- Go Cheat Sheet: https://github.com/alichator/golang-cheat-sheet

Communication

Important course information will be sent through Piazza and the course page here will be updated to reflect that information. Piazza is the best method to contact instructor, however if you must email please start the subject line with [PracticalCrypto] to make it easier to find. We will try to respond to questions within 48 hours, though we hope to make this more prompt with the hiring of additional course support staff.

Course Schedule

January 22: Introduction

- Reading: Boneh/Shoup Textbook, Chapter 2, from chapter start through the end of Section 2.1

January 24: Intro to Cryptographic Primitives I (Symmetric key crypto)

- Reading: Boneh/Shoup Textbook, Chapter 2, Sections 2.2 through 2.2.2 and section 2.3.1
- Assignment 1 is released (Due February 8)

January 29: Intro to Cryptographic Primitives II (Symmetric key crypto continued)

- Reading: Boneh/Shoup Textbook, Chapter 3, beginning of chapter through Section 3.3

January 31: Intro to Cryptographic Primitives III (Symmetric key crypto continued)

- Reading: Boneh/Shoup Textbook, Section 3.6, Sections 3.8 and 3.9

February 5: Intro to Cryptographic Primitives IV (Public-key crypto I)

- Project Proposals (Due February 14)
- Reading: Boneh/Shoup Textbook, Appendix A (Basic Number Theory)

February 7: Intro to Public Key Crypto Mathematics

Electronic Stuff & Reading

A Graduate Course in Applied Cryptography

Dan Boneh and Victor Shoup

Version 0.6, Jan. 2023

Electronic Stuff & Reading

- Website
  - https://github.com/matthewdgreen/practicalcrypto2024
    or my home page http://spar.isi.jhu.edu/~mgreen/
    (and click on the link for this class)
  - Slides up as we go
  - Reading assignment today (for Weds)
    Boneh/Shoup textbook (Chapter 2, through section 2.2)
  - My Office Hours Weds 1-3pm (provisionally), TA Office Hours (TBD but soon)
  - Assignment 1 out Weds
  - **Join the Piazza**

Programming

- The assignments in this class involve writing code
  - We will primarily use Go (with exceptions)
  - It's your responsibility to give us working assignments that build/run
  - Anything other than a working assignment is a failure

Course Guidelines

- Do:
  - Read the news!
    Twitter :(, Mastodon, Hacker News, Reddit r/netsec, ArsTechnica, etc.
  - Bring up interesting topics & recent attacks
    you'd like to learn more about
- Don't:
  - Cheat***
  - Get me arrested

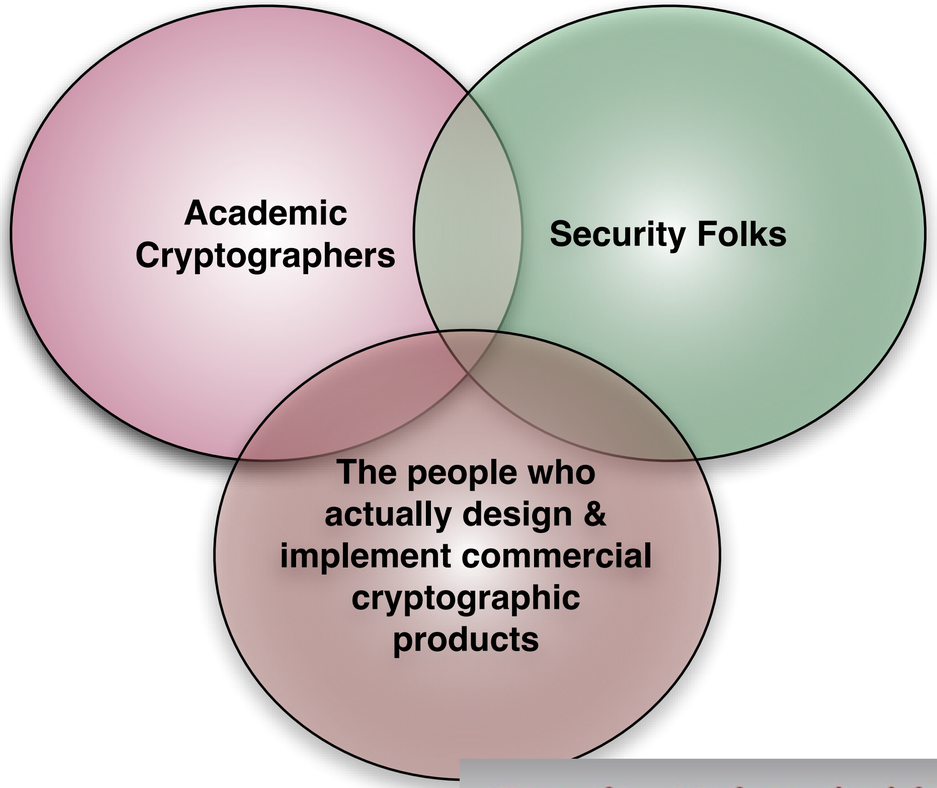
Readings

- Assigned each week
  - You must read them, be prepared to discuss in class
  - These wil be covered in written assignments on the homework, as well as exams

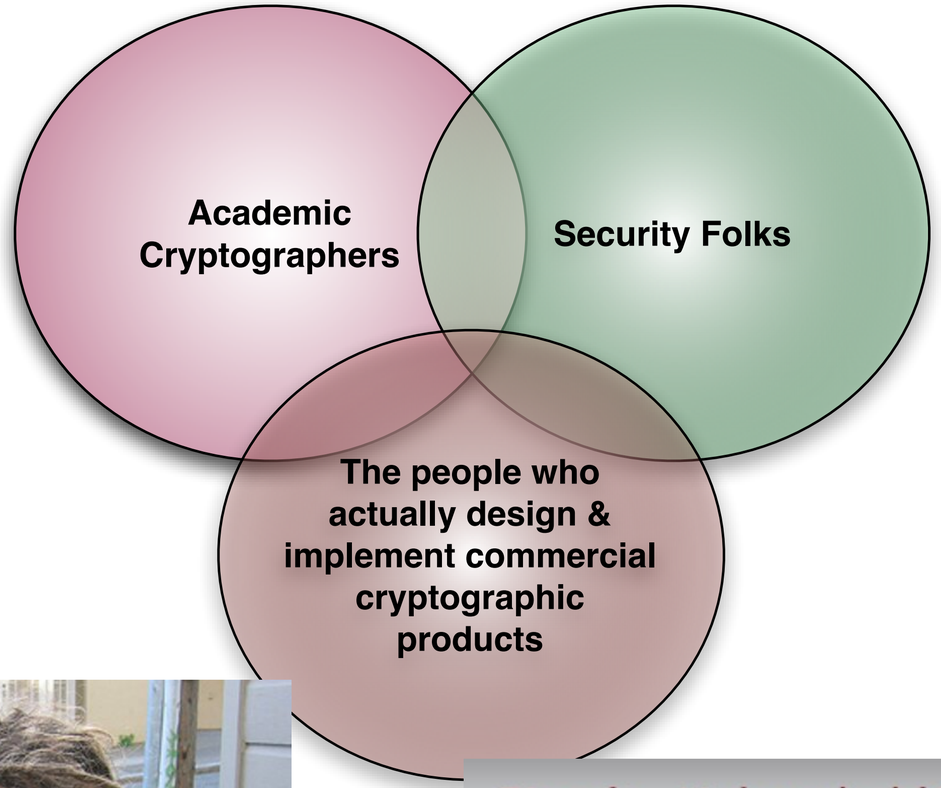
Written Homework

- Assigned many weeks
  - Based on readings
  - Graded probabilistically

Today


Academic
Cryptographers
Security Folks
The people who
actually design &
implement commercial
cryptographic
products


Simple, Unbreakable Encryption.


Academic
Cryptographers
Security Folks
The people who
actually design &
implement commercial
cryptographic
products


Simple, Unbreakable Encryption.

Security Failure

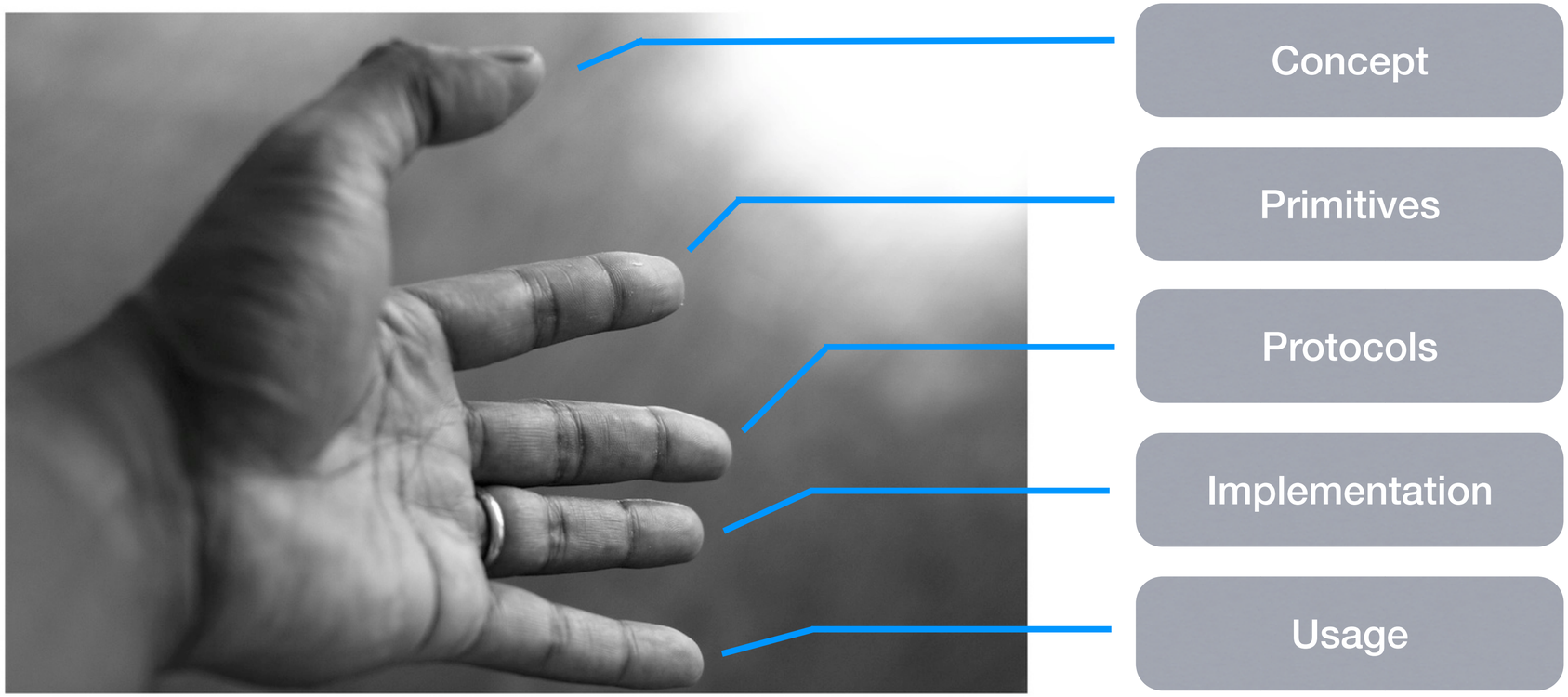
- When systems fail:
  - Researchers get published
  - $$$ lost
  - Private information compromised
  - People die (2)

Two arrested for stealing Jeeps -- using laptops

KHOU-TV 10:31 p.m. EDT August 4, 2016

HOUSTON – Police say charges have been filed against two suspects believed to be responsible for the theft and illegal export of more than 100 vehicles -- using laptop computers.

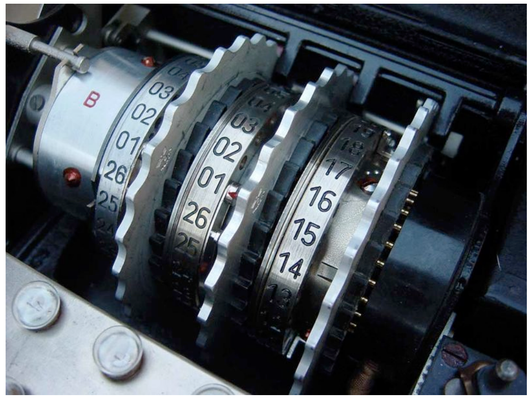
POPULAR USA TODA

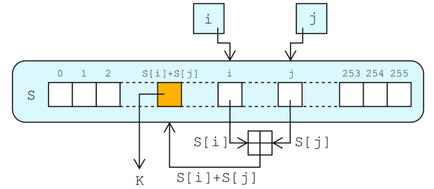

Concept
Primitives
Protocols
Implementation
Usage

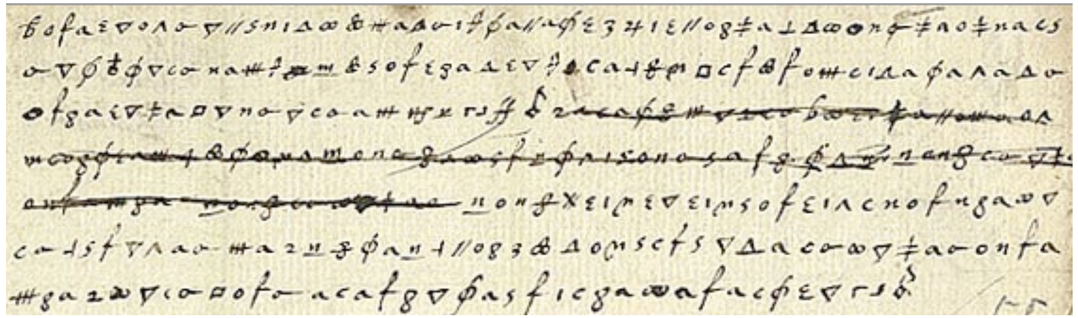
Primitives

Primitives

- Codes, ciphers, encryption schemes, MACs, etc.:
  - Classically, an attack on the “system” meant an attack on the primitive
  - History is littered with broken primitives





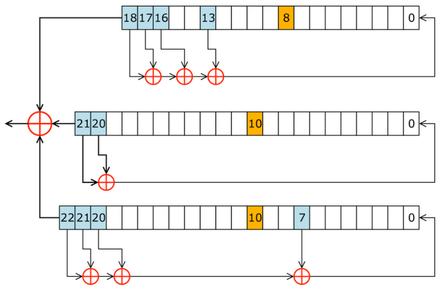


Primitives

- Practical Example: GSM encryption
  - A5/0: No encryption
  - A5/1: Based on LFSRs
  - A5/2: Weakened A5/1
  - A5/3 (KASUMI): New for 3G

GSM™
The wireless evolution

T-Mobile



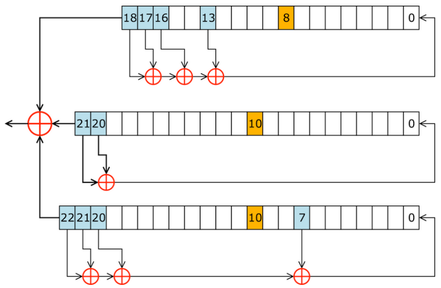
at&t

Primitives

- Practical Example: GSM encryption
  - A5/0: No encryption
  - A5/1: Broken
  - A5/2: Way Broken
  - A5/3 (KASUMI): Dented
    (and 3G vuln. to protocol attacks)
- Deliberately weak cipher design
  - Cost & politics

GSM™
The wireless evolution

T··Mobile



at&t

Primitives

- Practical Example: GSM encryption
  - A5/0: No encryption
  - A5/1: Broken
  - A5/2: Way Broken
  - A5/3 (KASUMI): Dented
    (and 3G vuln. to protocol attacks)
- Deliberately weak cipher design
  - Cost & politics

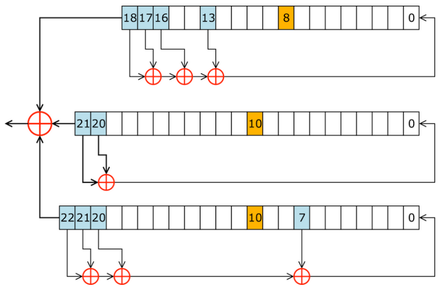
The New York Times

Cellphone Encryption Code Is Divulged

By KEVIN J. O'BRIEN
Published: December 28, 2009

BERLIN — A German computer engineer said Monday that he had deciphered and published the secret code used to encrypt most of the world's digital mobile phone calls, saying it was his attempt to expose weaknesses in the security of global wireless systems.

T-Mobile



at&t

Primitives

- Practical Example: GSM encryption
  - A5/0: No encryption
  - A5/1: Broken
  - A5/2: Way Broken
  - A5/3 (KASUMI): Dented
    (and 3G vuln. to protocol attacks)
- Deliberately weak cipher design
  - Cost & politics

threatpost

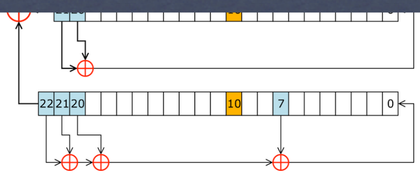
The Kaspersky Lab Security News Service

January 11, 2010, 4:57PM

A Second GSM Cipher Falls

A group of cryptographers has developed a new attack that has broken Kasumi, the encryption algorithm used to secure traffic on 3G GSM wireless networks. The technique enables them to recover a full key by using a tactic known as a related-hey attack, but experts say it is not the end of the world for Kasumi.

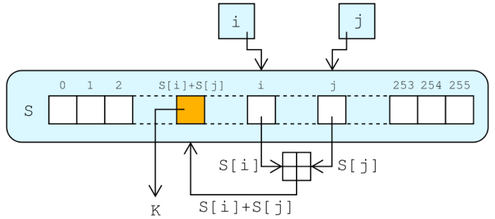
T-Mobile

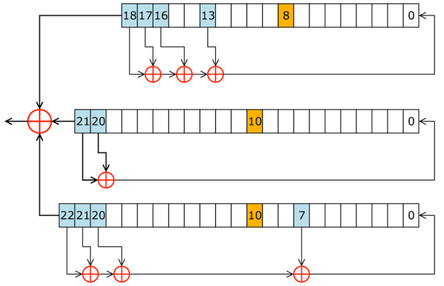


at&t

Primitives

- Typical problems:
  - Using the wrong ones (& homebrew crypto)
  - Or using the right ones... wrong
  - E.g., RC4 in WEP and TLS

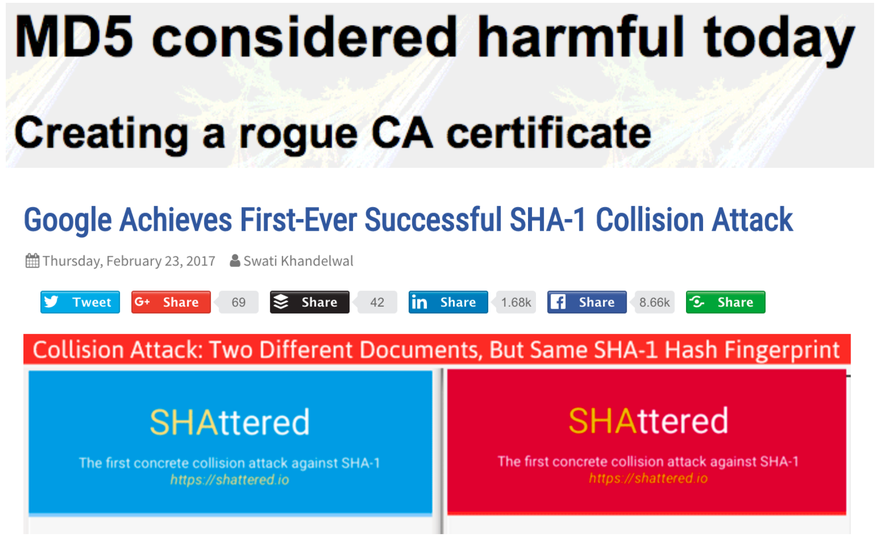




Virtual Matrix Encryption (VME) is a data security method and apparatus that provides an exceptional degree of security at low computational cost. The data security arrangement differs from known data security measures in several fundamental aspects. Most notably, the content of the message is not sent with the encrypted data. Rather, the encrypted data consists of pointers to locations within a virtual matrix, a large (arbitrarily large), continuously-changing array of values.

Primitives

- Sometimes the “right” primitives stop being right...
  - The great Hash Function Adventure of 2000-2017 (MD5 broken, SHA1 broken)



Primitives

- Sometimes the “right” primitives stop being right...
  - Mo

RC4 in TLS is Broken: Now What?

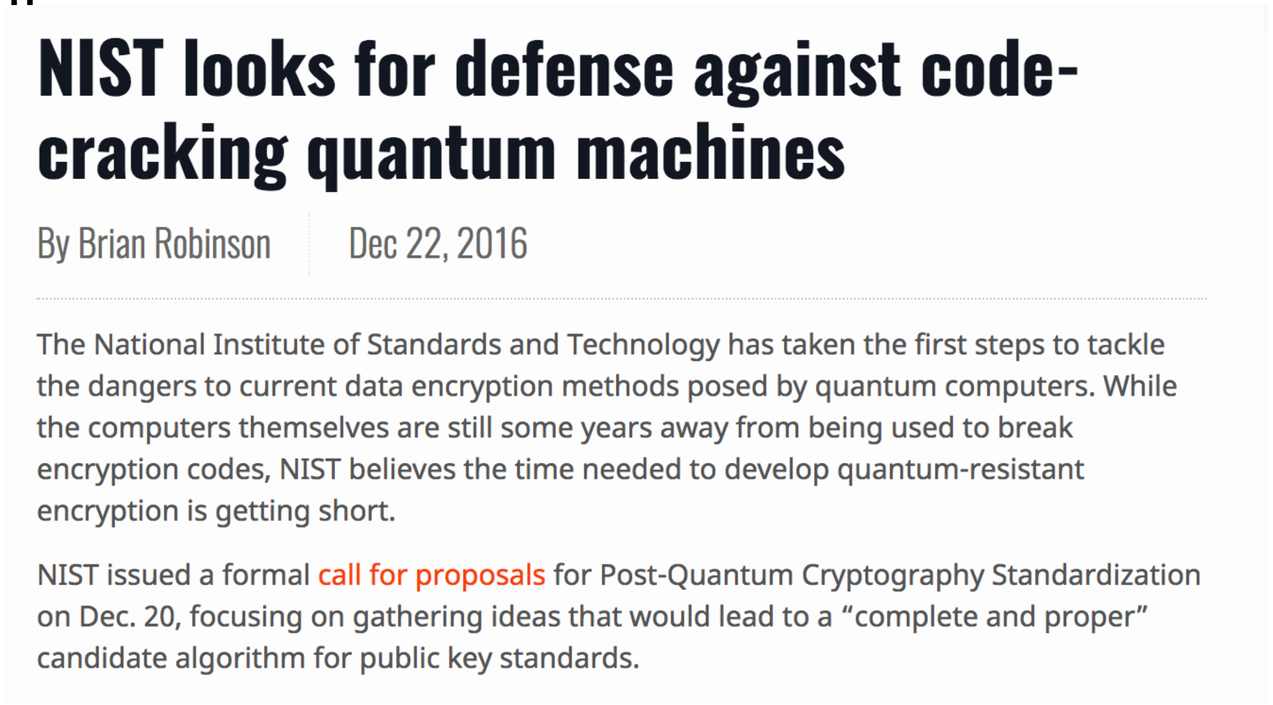
Posted by Ivan Ristic in SSL Labs on March 19, 2013 5:32 AM

RC4 has long been considered problematic, but until very recently there was no known way to exploit the weaknesses. After the BEAST attack was disclosed in 2011, we—grudgingly—started using RC4 in order to avoid the vulnerable CBC suites in TLS 1.0 and earlier. This caused the usage of RC4 to increase, and some say that it now accounts for about 50% of all TLS traffic.

Last week, a group of researchers (Nadhem AlFardan, Dan Bernstein, Kenny Paterson, Bertram Poettering and Jacob Schuldt)

Primitives

- Sometimes the “right” primitives stop being right



NIST looks for defense against code-cracking quantum machines

By Brian Robinson Dec 22, 2016

The National Institute of Standards and Technology has taken the first steps to tackle the dangers to current data encryption methods posed by quantum computers. While the computers themselves are still some years away from being used to break encryption codes, NIST believes the time needed to develop quantum-resistant encryption is getting short.

NIST issued a formal call for proposals for Post-Quantum Cryptography Standardization on Dec. 20, focusing on gathering ideas that would lead to a “complete and proper” candidate algorithm for public key standards.

Protocols

Protocols

- Classical cryptographic protocol:

Protocols

- Modern cryptographic protocol:

Protocol examples:

- Vehicle remote control/immobilizer
  - Only legitimate owner can start the car/ unlock the doors, etc.

Protocol examples:

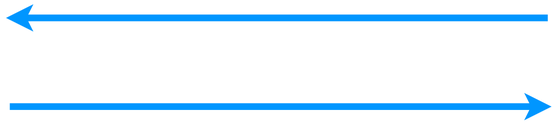
- Vehicle remote control/immobilizer
  - Early systems used fixed Serial Number

Protocol examples:

- Vehicle remote control/immobilizer
  - Early systems used fixed Serial Number
  - Vulnerable to “replay attack”

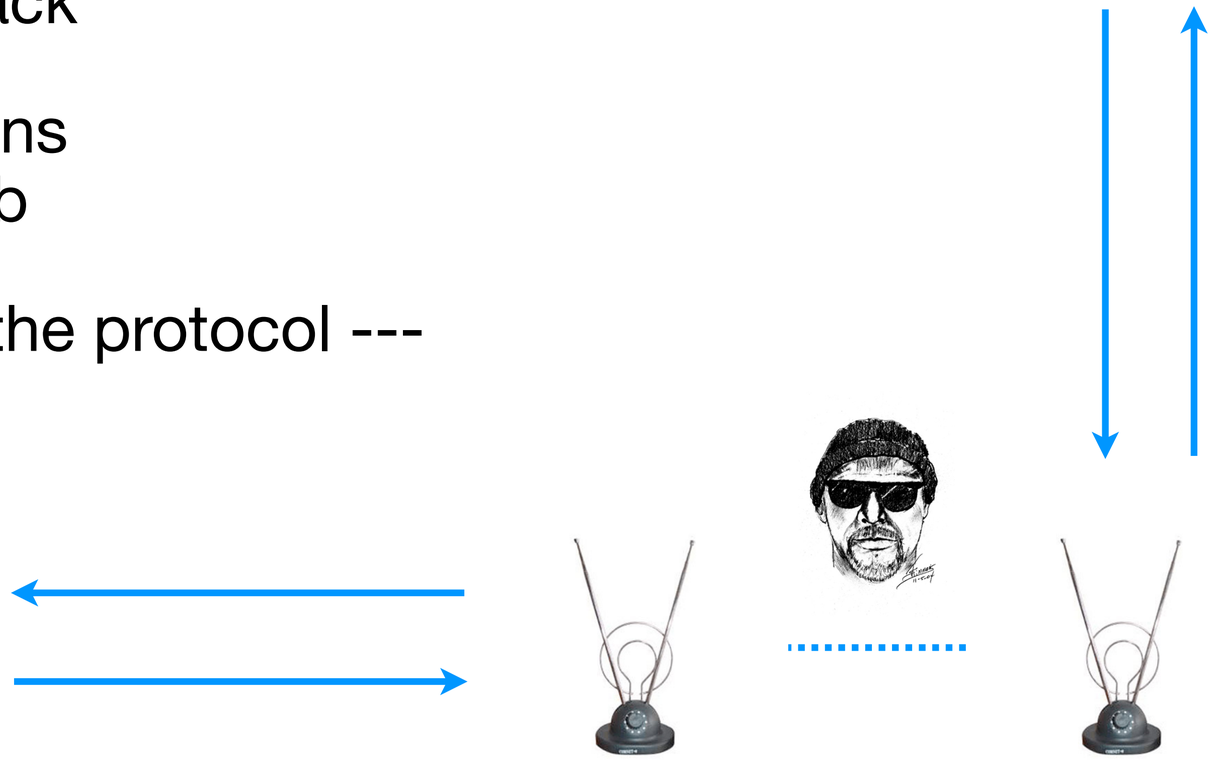
Protocol examples:

- Solution: Challenge-Response
  - “Identification Friend or Foe”
  - Key is never broadcast over the air



MITM

- Man in the Middle Attack
  - Route communications between car & keyfob
  - Don’t have to break the protocol --- just abuse it

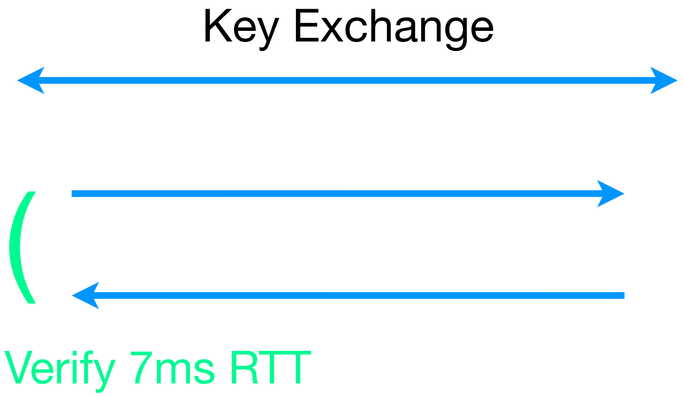


MITM

- Not just theoretical...
  - Anderson [Chap 2]
  - Military radars use a similar technique to identify friendly aircraft
  - How do we fix?

Round Trip Timing

- The case of DTCP-IP
  - Content transport protocol
  - Concern: prevent user from sharing content over the Internet



Round Trip Timing

Establish Shared Key K

For attempt N = 0 to 1023

N, C = HASH1(K | N)

R = HASH2(K | N)

Check that R= HASH2(K + N)
and response time within 7 ms
(If not, retry)

Check that C = HASH(K | N)

This check happens
way too late!

Implementation

Implementation

- Sadly, this is where most systems fail
  - Particularly if they're software-based

Oracle Security Alert #37
Created: 1 August, 2002
Updated: 5 August, 2002
Updated: 9 August, 2002
Updated: 24 September, 2002

OpenSSL Security Vulnerability

Description:

There are remotely exploitable buffer overflow vulnerabilities in OpenSSL versions prior to 0.9.6e.
These vulnerabilities may allow a remote attacker to execute arbitrary code or perform a denial-of-service (DoS) attack.

CONSOLE HACKING 2008: WII FAIL
Is implementation the enemy of design?

marcan and bushing
Team Twiizers

⚠ Vulnerability in Citrix Presentation Server could result in cryptographic settings not being correctly enforced

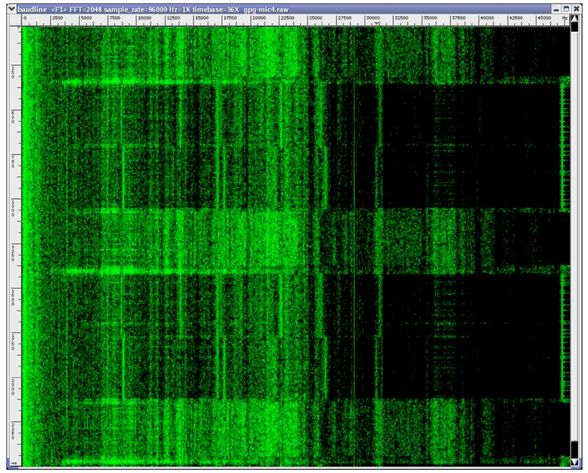
Implementation

- Typical problems:
  - Poor protocol implementation
  - Bad PRNGs
  - Software vulnerabilities
  - Untrusted platforms
  - Side channel attacks
  - Weak hardware
  - Deliberate backdoors

KIM ZETTER SECURITY 01.08.16 7:00 AM

NEW DISCOVERY AROUND JUNIPER BACKDOOR RAISES MORE QUESTIONS ABOUT THE COMPANY

USN-612-2: OpenSSH vulnerability



Software

- Routine coding errors
  - Use strcmp() instead of memcmp()
  - Don’t check your buffer bounds
  - Don’t check your malloc() responses
  - Code anything secure on Windows
  - Write your own OpenSSL
  - Use the real OpenSSL...

Software

- Routine coding errors
  - Use strcmp() instead of memcmp()
  - Don’t check your buffer bounds
  - Don’t check your malloc() responses
  - Code anything secure on Windows
  - Write your own OpenSSL
  - Use the real OpenSSL...

Software

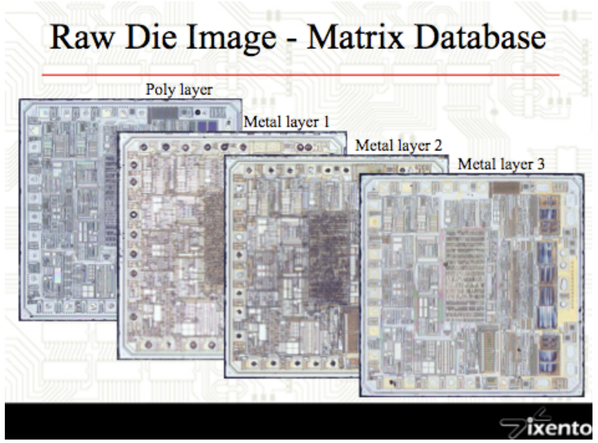
- More sophisticated issues
  - Which cryptographic libraries to use?
  - How to manage keys?
    (hint: not like this)

```
#define DESKEY ((des_key*)"F2654hD4")
```

  - Will keys be booted out into swap?

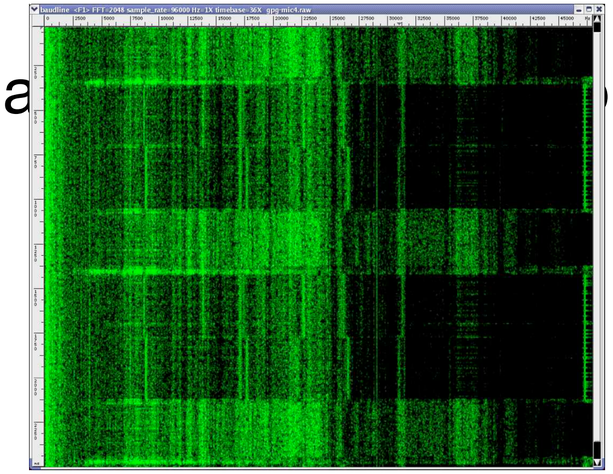
Hardware

- May lead to a false sense of security
  - The notion that the bad guys can’t crack open/reverse engineer your system
- Tamper-evidence
  - Detect malicious activity
- Tamper-Resistance
  - Better
  - Depends on who’s tampering, and how.



Side-Channel Attacks

- Even when perfectly implemented
  - System can leak information through a “side channel”:
    EM, power consumption, audio, timing
  - Across a VM or process boundary
  - E.g., recovering RSA keys via low-bandwidth a hone!



Usage

Usage

- Unfortunately, users may be your greatest foe
  - Weak password choices, refusal to change defaults
  - Insistence on backdoors, fail-open mechanisms
  - Loss of key material, data
  - And so far we're talking about the honest users!

Usage

- Unfort
  - Wea
  - Insis
  - Loss
  - And

POLITICS 12/05/2013 02:13 pm ET | **Updated** Jan 23, 2014

‘Secret’ Nuclear Missile Launch Code During Cold War Was ‘00000000’

By Ryan Grenoble

SPACES IMAGES VIA GETTY IMAGES

TRENDING

Usage

- Insider attacks:
  - Almost impossible to deal with
  - Ultimately relies on policy, vigilance
  - Where possible:
  - minimize trust
  - provide for system renewability

Concept

Concept

- Certain things cannot be done
  - Perfect (software) DRM
    (i.e., user can watch/play/use the encrypted content, but can't decrypt it themselves)
  - Cryptographic software obfuscation
    (general case)
- Ok, if you understand:
  - These systems can at most slow down the attacker
    an attac

Studios' DVDs Face a Crack in Security

By JOHN MARKOFF
Published: January 1, 2007

SAN FRANCISCO, Dec. 31 — An anonymous computer programmer may have skewed the competition over standards for high-definition DVD discs by possibly defeating a scheme that both sides use to protect digital content.

DirecTV zaps hackers

Kevin Poulsen, SecurityFocus 2001-01-25

Wednesday, Aug

Electronic warfare tactics wipe out thousands of hacked smart c

Microsoft Patches DRM Hack

Microsoft has responed to an application that threaded to remove the DRM encoding from Windows Media Files, and released a security patch.

Enthusiasts website *Engadget.com* had reported on a small utility called FairUse4WM able to remove DRM information from WMA files to allow playback on any device.

Kerckhoffs’ Principle(s)

- Auguste Kerckhoffs (1835-1903)

Kerckhoffs' Principle(s)

2. It must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience;

"The enemy knows the System"
-- Claude Shannon's Maxim

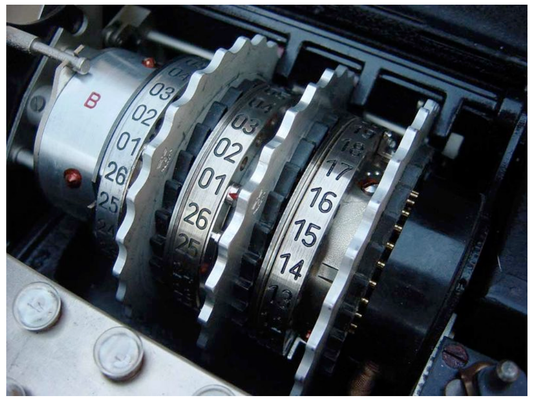
Don’t worry!

- I’m not all doom & gloom
  - We can do some things very well
  - Other things fairly well
  - Still others… well-ish
- We can certainly do better than most

Going forward:
The next few weeks

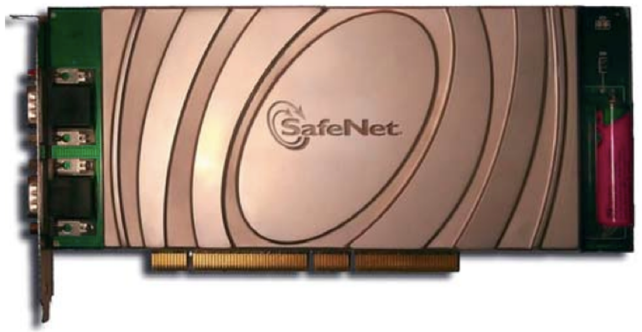
Part 1

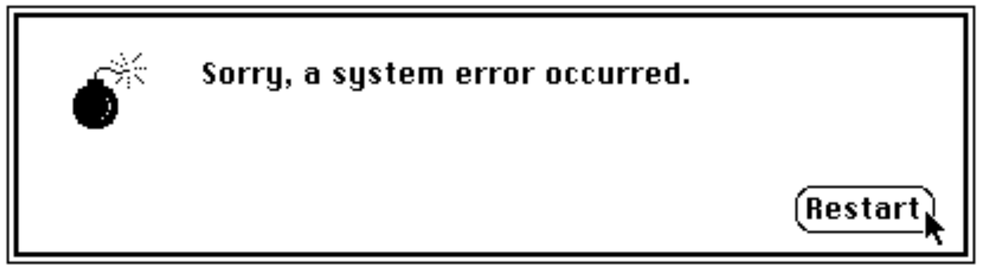
- Introduction to Crypto... at high speed:
  - Classical cryptography
  - Symmetric-key encryption & block ciphers
  - DES, the modes of operation
  - Public-key cryptography
  - Diffie-Hellman, RSA



Part 2

- Exploiting Software:
  - Corrupting, overflowing and generally messing with software systems
- Physical security
  - Tamper-resistance
  - Hardware Security Modules
  - Fault attacks





Part 3

- Reductionist security & protocols
  - Proving the security of a construction
  - Analyzing protocols that fail
- Random number generation
- Security evaluation
  - What a security evaluation process looks like
  - The FIPS standards

A Note on Ethics

- We'll be discussing vulnerabilities in many systems
  - Some have been fixed
  - You might find more
  - It goes without saying: exploiting systems is often a crime. Be careful.
  - Important to disclose vulnerabilities responsibly

END