CS 465 Winter 2022 Mid-Term Exam 1 Study Guide

Administered by the BYU Testing Center. Closed book/internet. Simple Calculator allowed, but probably not needed. (please no notes/algorithms/info saved in your 90's technology calculator). One 8.5 inch by 11 Inch sheet of paper with hand-written notes (both sides) allowed.

Expected time is 60 to 120 minutes, there is no time limit. For the written answer questions: Answer each question as completely as possible.

20 multiple choice questions - 3 points each
5 'long answer' 5-10 points each, show your work. 100 points total.
Tuesday through Thursday, in the Testing Center.

Basics of crypto: Goals:

- Access Control (authentication, authorization)
- Confidentiality
- Integrity
- Non-repudiation.
- Forward Secrecy

Basics of crypto: Real-world-application:

- Defense in depth
- Security Minded (healthy paranoia)
- Use public algorithms, hardened implementations
    - Which are considered 'secure' today

- Assume kerckhoffs principle is your guide. Know what kerckhoff's principle is!

AES:

- how GF are represented as a polynomial and as a {bitfield}
- Details of GF operations you worked on
- **requirements for strong symmetric encryption:**
- Strong/Safe key exchange and storage
- addition, subtraction, xtime, FF-multiply,
- (NOT internals of of the diffusion functions)

Block Modes and Stream Ciphers:

- Block vs. Stream ciphers
- Block-cipher modes
- Relative strengths, weaknesses
    - Recoverability in the face of data corruption
    - Parallelization
- The role of IV (nonce) and how to include in crypto systems
- How to read an encryption diagram
- Padding
    - When?
    - Why?
    - How?
    - Short blocks and padding?

    - Other than block size, reasons to pad?
- Authenticated Encryption Modes
    - How are they different from normal encryption?
    - What additional security properties do they offer?
    - What additional crypto constructs are used (besides AES)?

Hash functions:

- Properties of an ideal hash
- Types of attacks against hashes and relative effort
- Uses of cryptographic hashes

MAC/HMAC:

- What cryptographic guarantees do they provide?
    - Integrity and authentication
    - Not confidentiality, Not Nonrepudiation
- **Multiple** Methods of implementation
- Inputs/Outputs of a MAC
- Length extension attack details
    - Make sure you understand what you did on project in detail
- Understand HMAC formulation as described in lecture material. How does it prevent extension attacks?
- What is the recommended secure implementation of a MAC from NIST?

Public-key Crypto:

- Diffie-Hellman, RSA
- By-hand DH key exchange - know how it works, explain it to someone else step by step.
- Generating RSA parameters by hand using extended euclidean algo - Be prepared to do it - like in the homework

- Encryption versus Signatures
    - Mechanics of using RSA to do either
      What keys do you use for what operations?

- Real-world issues
    - Message size
    - Padding(how, why)
    - Choice of d,e (e.g. in hardware) (RSA e = 65537 almost universally - why?)
    - Why does a small public exponent not pose a risk? (either cryptanalysis or side-channel)

Certificates:

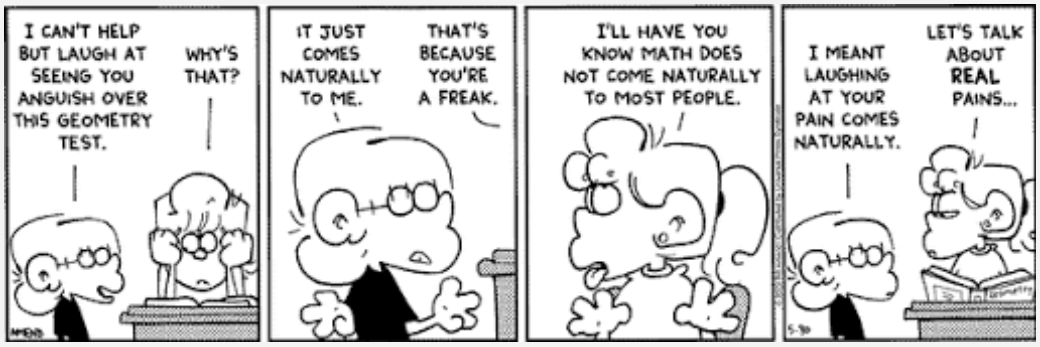
- How they are created - what steps are taken by which parties? Explain in detail to someone else
- Terminology of various entities in the system
- Certificate chaining

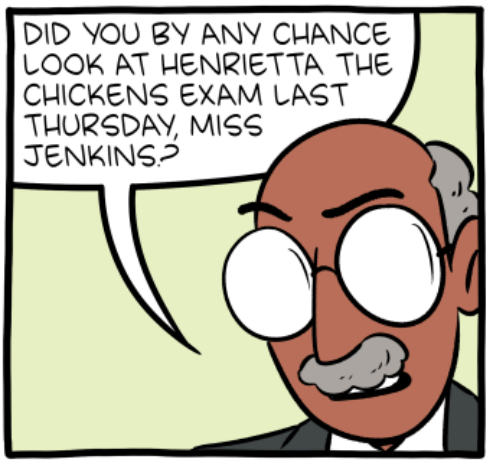
- Steps for certificate verification
- Revocation
- Trust issues

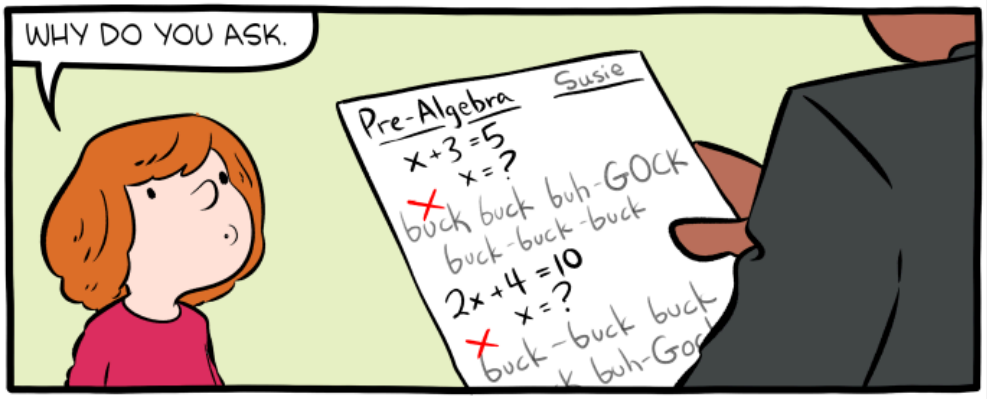
Algorithms:

- Make sure you know how the following Cryptographic algorithms are categorized (do they perform encryption, signatures, MAC, hash, and are they secure?)
    - AES
    - DES
    - MD5
    - SHA-1
    - SHA-2
    - SHA-3
    - RSA
    - MAC
    - HMAC

Comics for Professor Fred Clift







smbc-comics.com