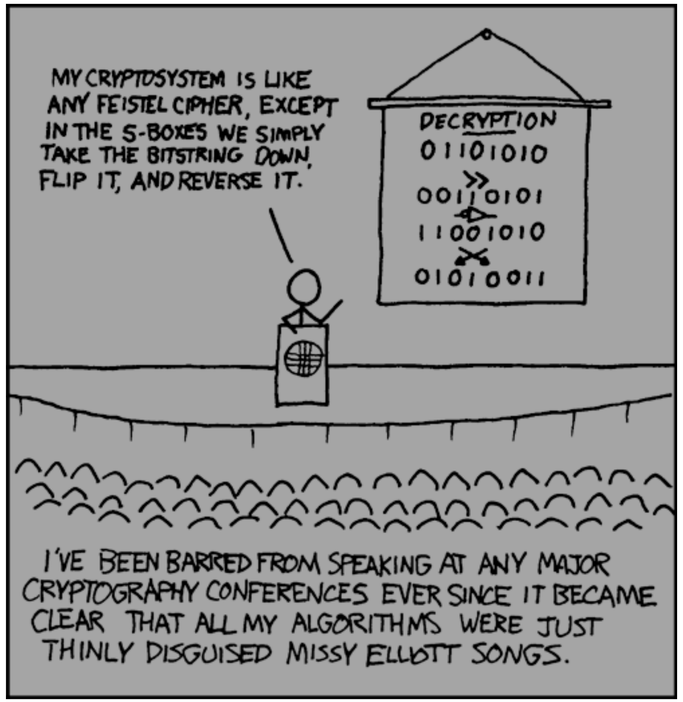
Cryptography (contd)



Review

- What type of encryption uses two keys instead of one?
- Which is faster, symmetric or asymmetric encryption?
- Is encoding the same as encryption?
- Should we use ECB or GCM?
- Should we use DES or AES?
- What is more important to protect, the private or the public key?
- Can we share the public key?

Quiz!

Review Assignment

Exercise - 10 Minutes

- Get in groups of 2 to 3
- Create a private/public key pair
- Email to the group member your public key
  - You can login from your VM to email or if you enabled an appropriate setting in your VM, copy and paste from the VM to your host OS
- Have them use your public key to send you a message (keep it appropriate)
- Test if you can decrypt the message using your private key
  - Give me a thumbs up if you got it to work!

Hashing

- One way "encryption"
  - Cannot reverse, but can still attack by testing hashed values
- Used to create a signature or "store" a password
- Can be used for integrity and confidentiality
- Popular algorithms:
  - MD5 - Don't Use
  - MD4 - Don't Use
  - SHA-0 - Don't Use
  - SHA-1 - Don't Use
  - SHA-2 - Can Use
  - SHA-256 - Should Use

Let's Try It Out!

- Open your VM

Digital Signatures

- Essentially: Hashes with asymmetric encryption
- You generate a hash from a message and then sign it with your private key
  - Receiver can verify by hashing the same message and using your public key to verify
- Used for non-repudiation, guarantees who sent the message

Storing Passwords

- Never **NEVER** store passwords in the clear
  - If a website can tell you what your password is, don't use that service!
- Popular algorithms:
  - Argon2id (should use)
  - PBKDF2 (can use)
  - Bcrypt (can use)

What Is Used in PHP?

- https://www.php.net/manual/en/function.password-hash.php

Steganography

- Not encryption, but relevant to this field
- Hiding data within other data sources
  - Changing bits in an image
  - Storing data within a video

Important

- Never write your own encryption
- Use what is proven and tested
- Stay up to date on the latest best practices and which ciphers should not be used

Recap

- What is faster, asymmetric or symmetric?
- Which one has a larger key size?
- Give the choice between the two, should you use use ECB or CBC?
- What is the difference between encoding and encryption?
  - Why would encoding still be used?
- What is a hash?
- How is hashing and encryption used in digital signatures?

Cryptography in Java

- Open IntelliJ (or an alternative Java IDE)
- You can work in groups of 2-3