Conclusions

Summary

- Applied cryptanalysis: attacks that produce plaintext and/or recover keys
- We studied applied attacks on…
- Classic ciphers
  - Transposition, substitution, linear ciphers, one-time pad, codebook, etc.
- WWII cipher machines
  - Enigma, Purple, Sigaba

Summary

- Stream ciphers
  - Shift registers, correlation attack, ORYX, RC4, PKZIP
- Block ciphers
  - Modes, MAC, Feistel cipher, Hellman's TMTO, CMEA, Akelarre, FEAL
- Cryptographic Hash functions
  - HMAC, birthday attacks, Nostradamus attack, MD4, MD5

Summary

- Public key systems
  - Overview of Knapsack, Diffie-Hellman, Arithmetica, RSA, Rabin, NTRU, ElGamal
- Public key attacks
  - Factoring algorithms: trial division, Dixon's algorithm, quadratic sieve
  - Discrete log algorithms: trial multiplication, baby step giant step, index calculus
  - RSA timing attacks: Kocher's, Schindler's, Brumley-Boneh
  - RSA glitching attack

Secure Ciphers

- There are many **secure** ciphers
  - No significant shortcut attack known
- Symmetric ciphers
  - Stream cipher: RC4 (when used properly)
  - Block cipher: AES
- Public key systems
  - RSA, Diffie-Hellman, etc.

Applied Cryptanalysis

- Many other ciphers where attacks are only theoretical
- In this course, you learned…
  - To analyze ciphers and attacks
  - To analyze algorithms, in general
  - Intro to cryptography
  - Foundation for further study