Introduction to Cryptography

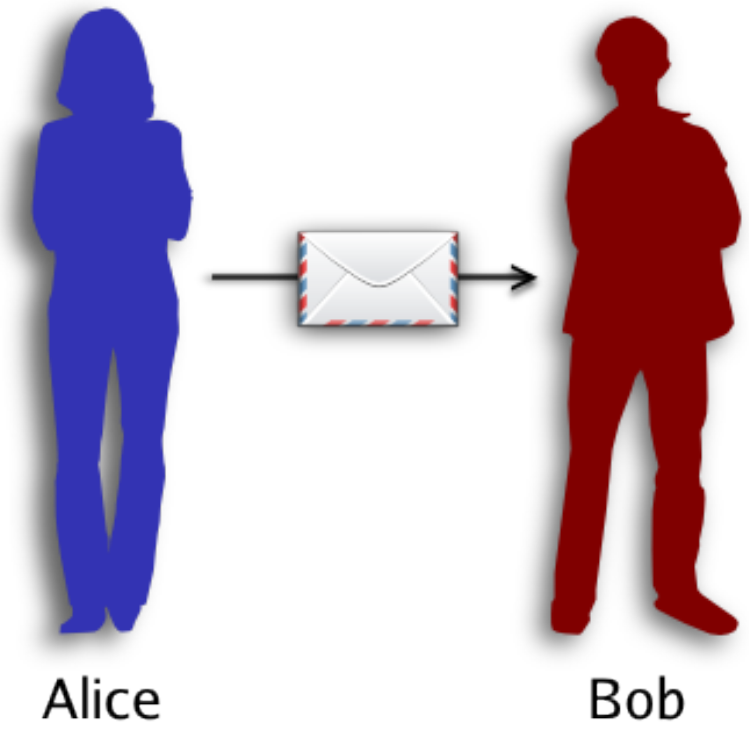
Tom Wheeler

What I'm Going to Cover

- What cryptography is and why it's important
- How historic and modern cryptography differ
- Main concepts behind several forms of cryptography

What is Cryptography

- The science of keeping information secret
- Essential when communicating in an insecure environment
- Confidentiality / message integrity

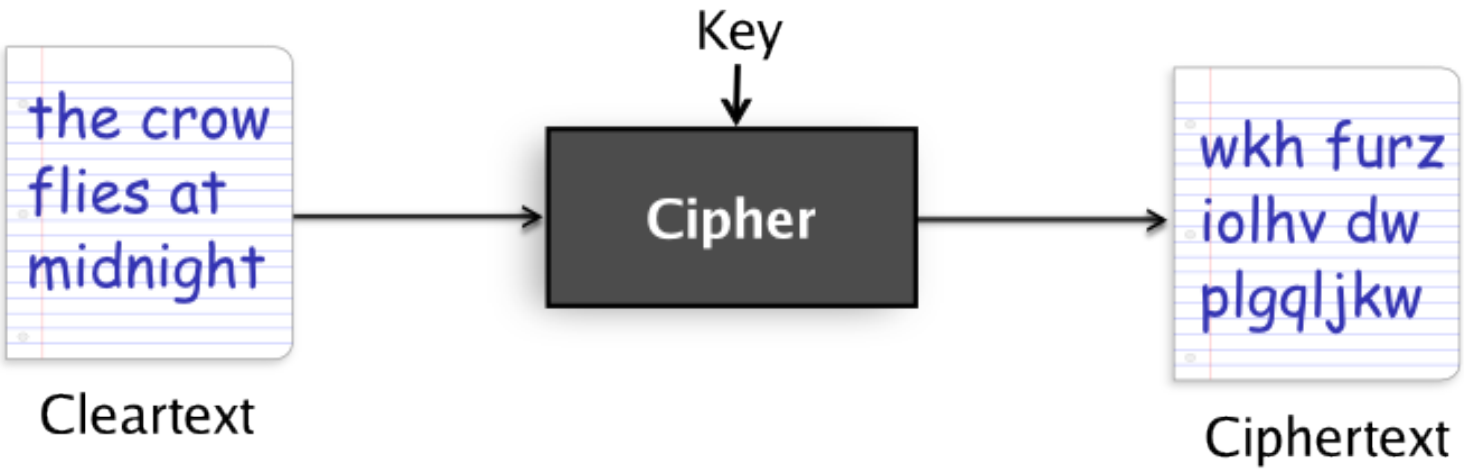


How is Cryptography Used

- Shopping on the Web
- Online banking
- Disk encryption
- Mobile phones
- Remote access systems (VPN, ssh)

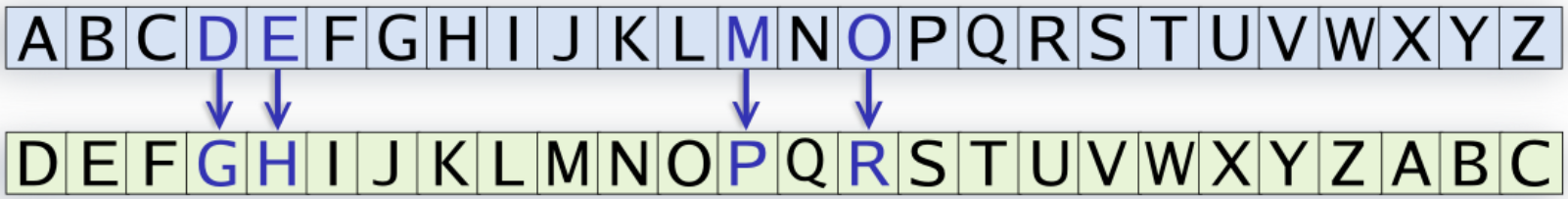
Encryption

- Encryption renders a message secret using a cipher
- **Input**: cleartext and key
- **Output**: ciphertext



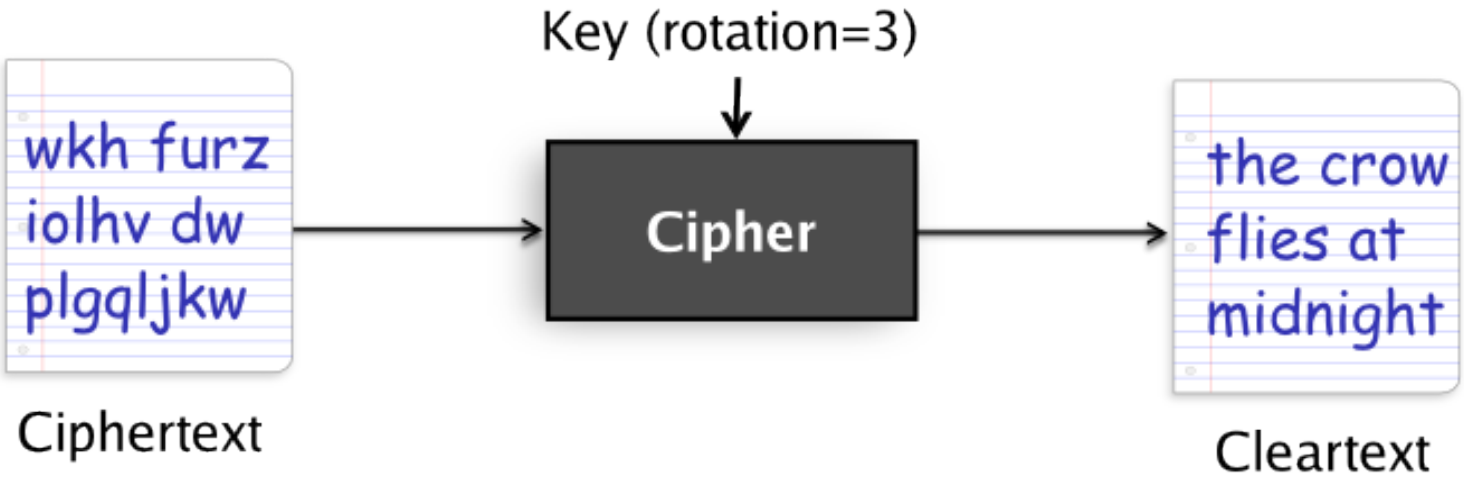
Encryption: Substitution Cipher Example

- Substitution ciphers are historically important
- Caesar cipher
- Maps a character to another (translation table is key)



Decryption

- Extracts the original message from ciphertext
- **Input**: ciphertext and key
- **Output**: cleartext

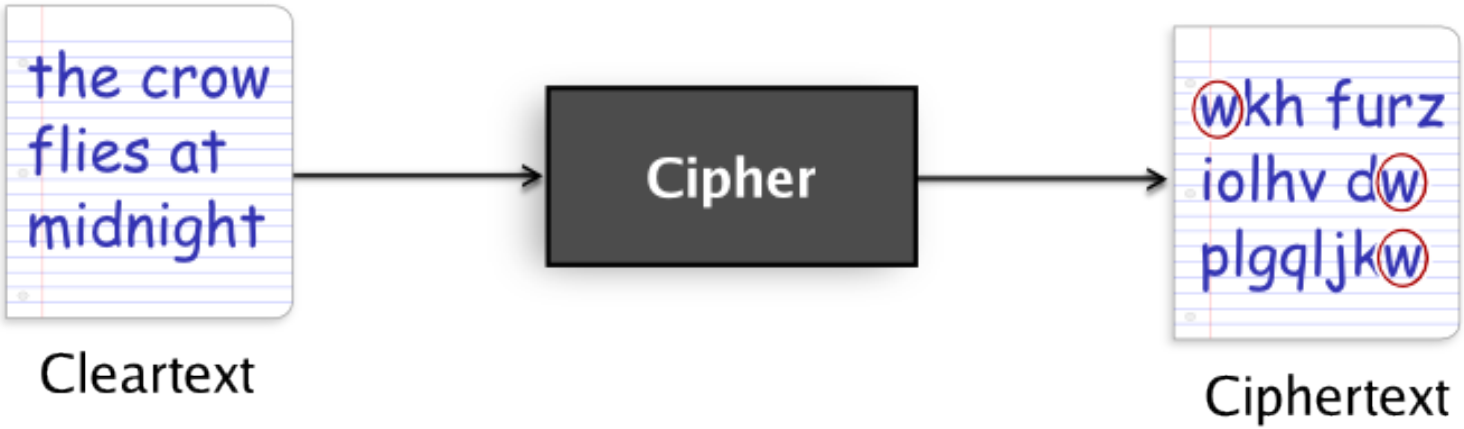


Review Terms

- **Cleartext**: original (readable) message
- **Ciphertext**: scrambled unreadable message
- **Cipher**: An encryption algorithm
- **Key**: Input parameter for cipher (e.g. password)

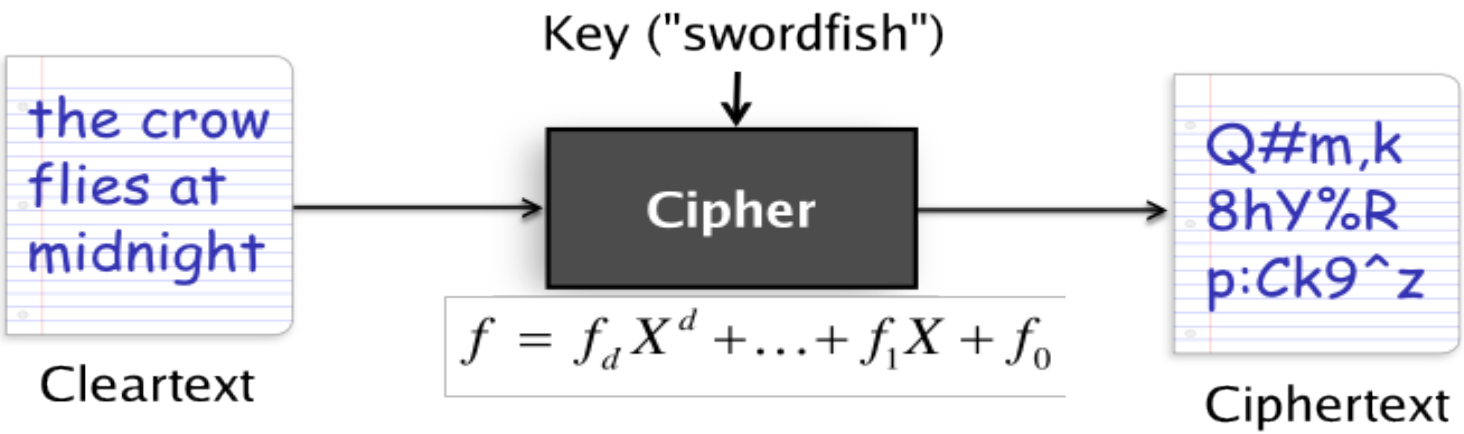
Cryptanalysis

- Substitution ciphers are linguistically-based
- Also defeated with linguistics: frequency analysis
- Advent of computing makes this trivial



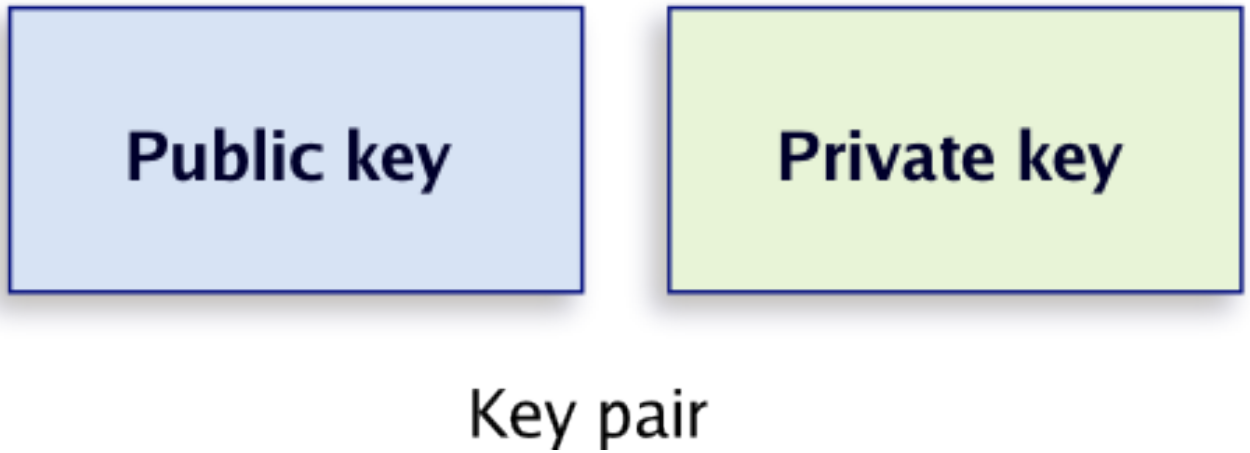
Modern Cryptography: Symmetric

- Complex math instead of simple substitutions
- Two main categories of modern ciphers
- #1: Symmetric (same key)
- **Question:** What is the disadvantage of this?



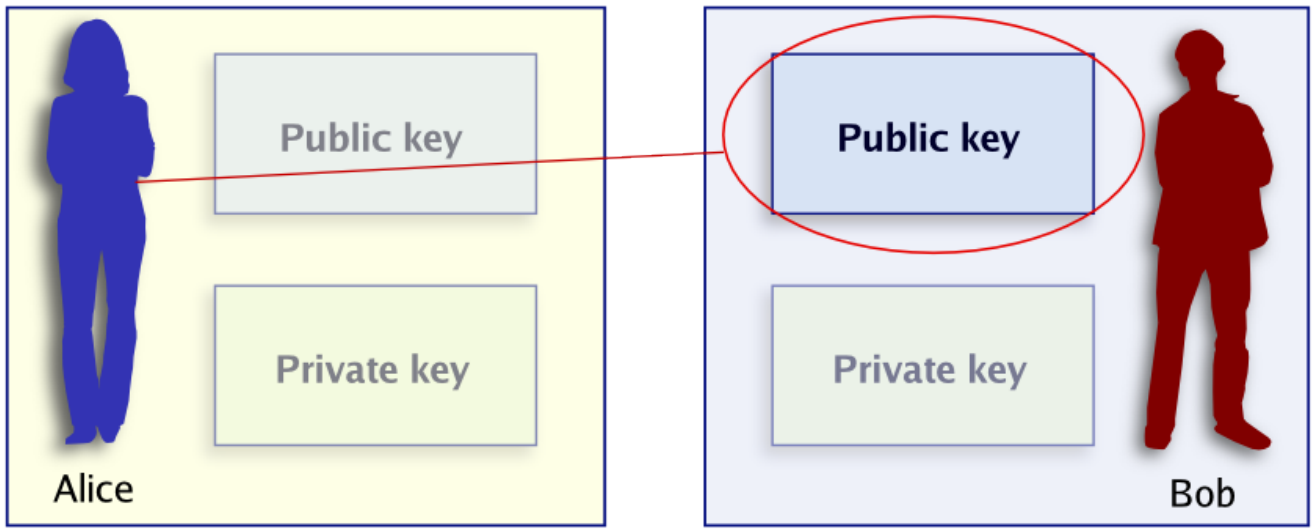
Modern Cryptography: Asymmetric

- #2: Asymmetric (uses a pair of keys)
- One used to encrypt (public)
- The other used to decrypt (private)



Asymmetric Cryptography: Encryption Example

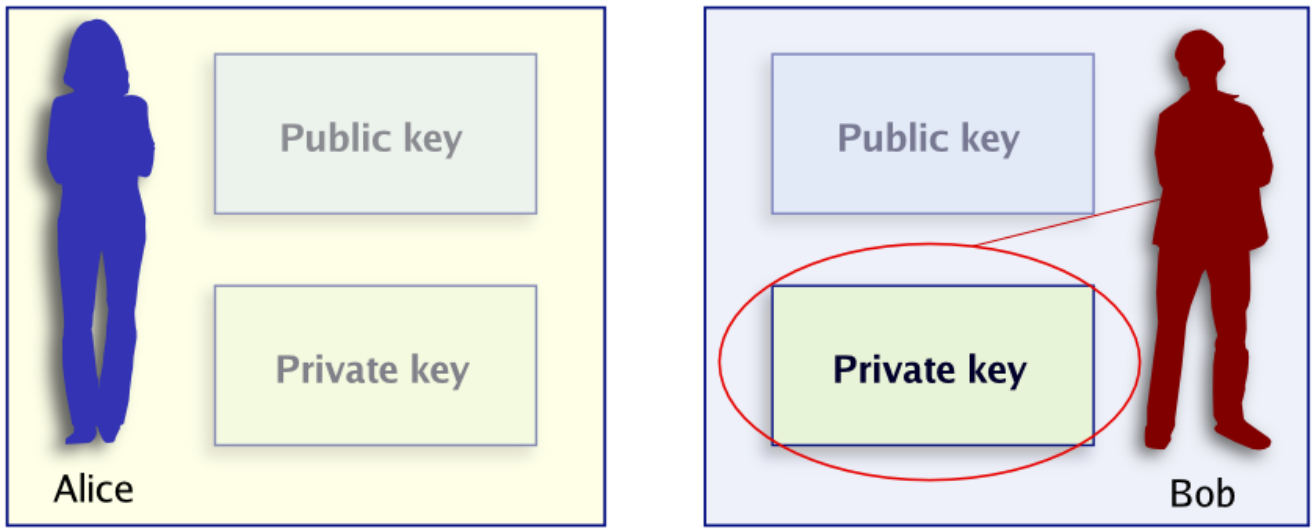
- Alice wants to send a confidential message to Bob
- She uses Bob's public key to encrypt



Alice encrypts a message for Bob using an asymmetric cipher

Symmetric Cryptography: Decryption Example

- Bob wants to read Alice's message
- He uses his private key to decrypt



Bob decrypts Alice's message using an asymmetric cipher

Review Questions

- Please name two ways in which you've used cryptography.
- How can a substitution cipher be defeated?
- What are the two main categories of ciphers?
- What's the main disadvantage of a symmetric cipher?

Conclusion

- Cryptography is essential to everyday modern life
- Cleartext is encrypted to form ciphertext
- Classical = linguistics / Modern = math
- Ciphers: symmetric and asymmetric

Thank You

- Any questions?