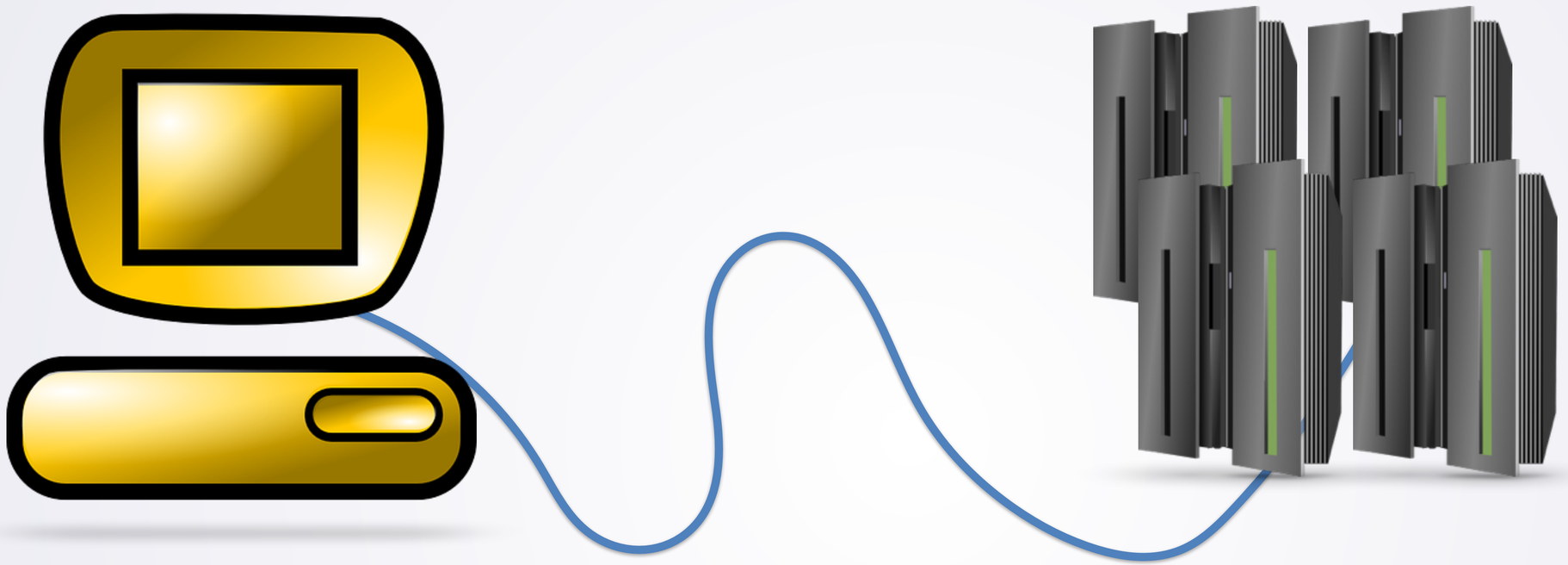
Implementing the Caesar Cipher

A Brief History of Cryptography

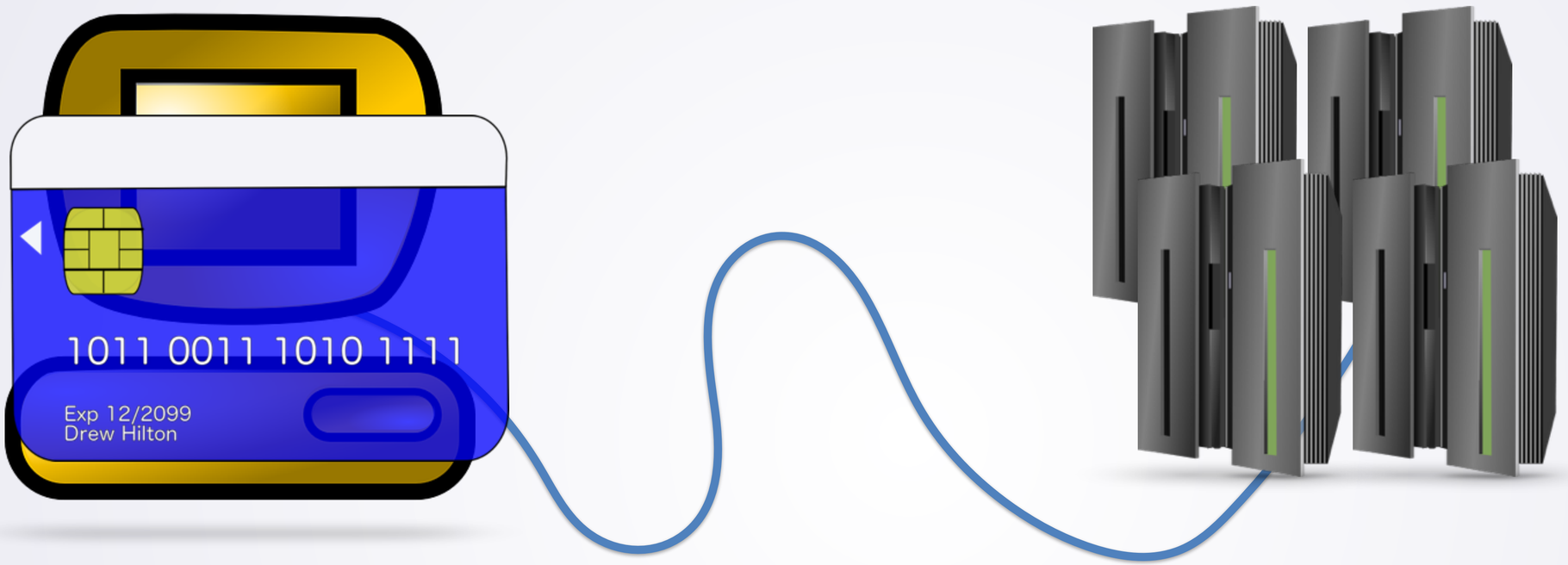
Duke
UNIVERSITY

Online Shopping: Security



- A little bit about computer security
- You want to buy something online

Online Shopping: Security

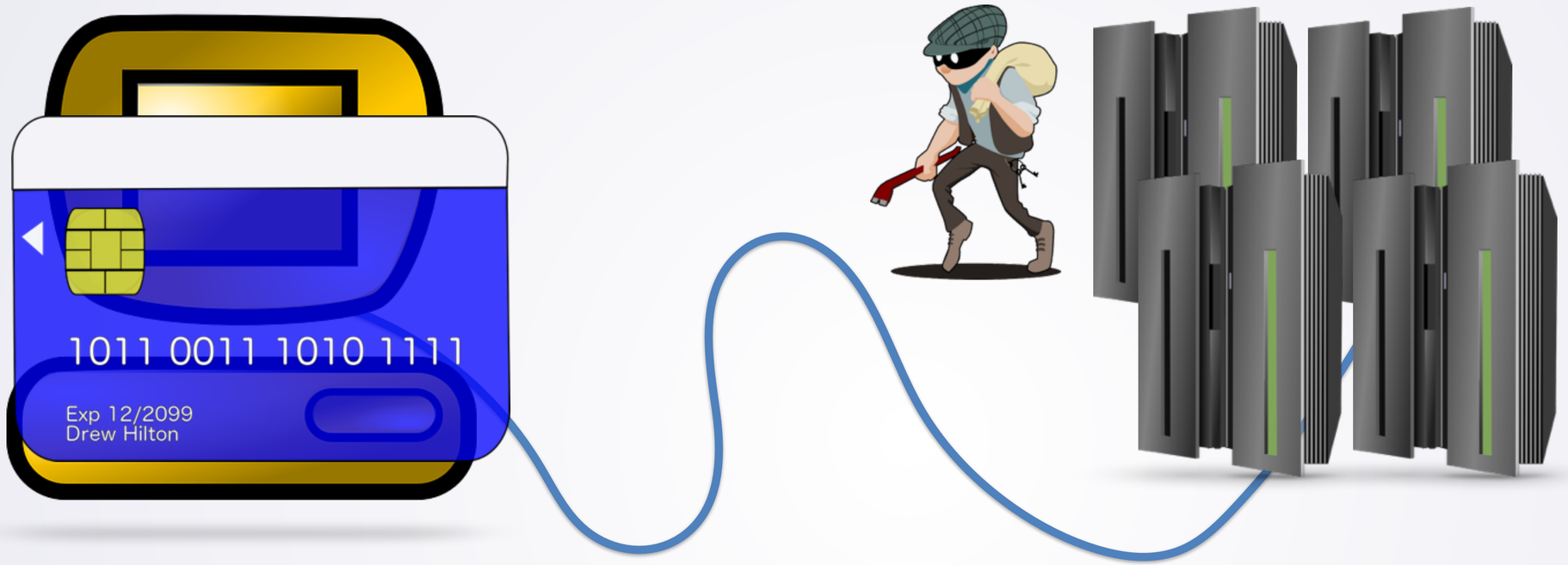


- A little bit about computer security
- You want to buy something online

Online Shopping: Security

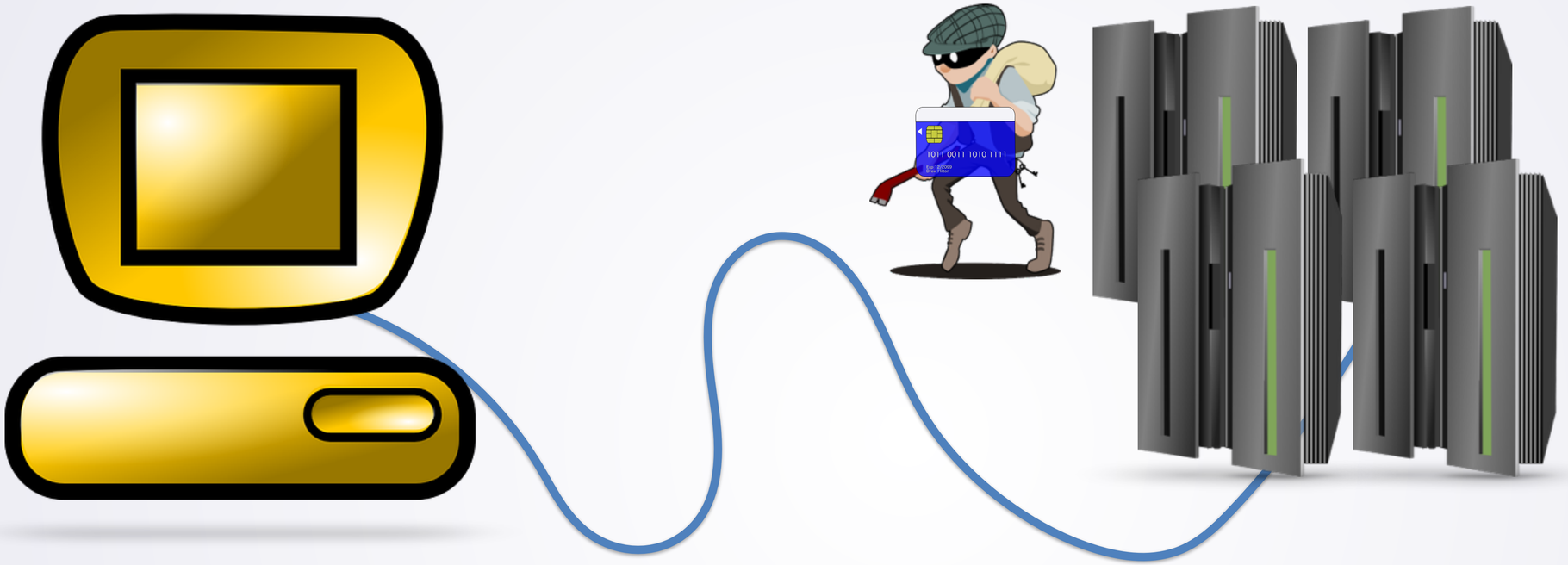
- A little bit about computer security
- You want to buy something online
  - Send credit card information to online store

Online Shopping: Security



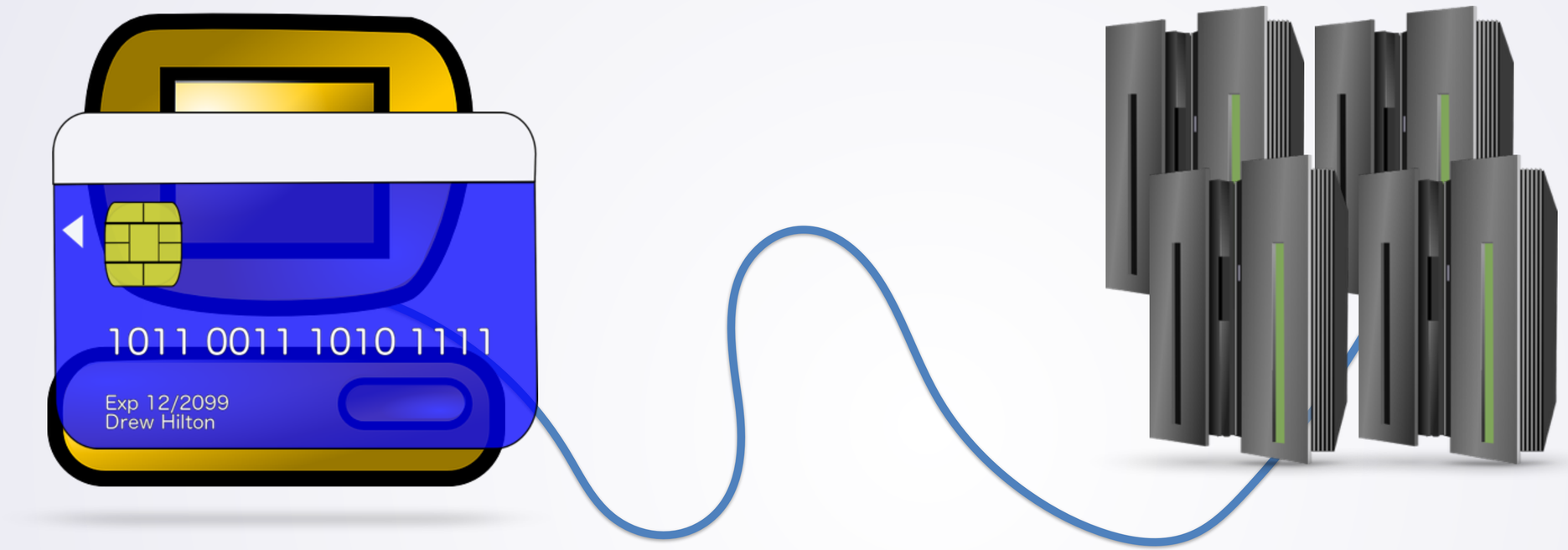
- You want to buy something online
  - Send credit card information to online store
- Do not want credit card info stolen

Online Shopping: Security



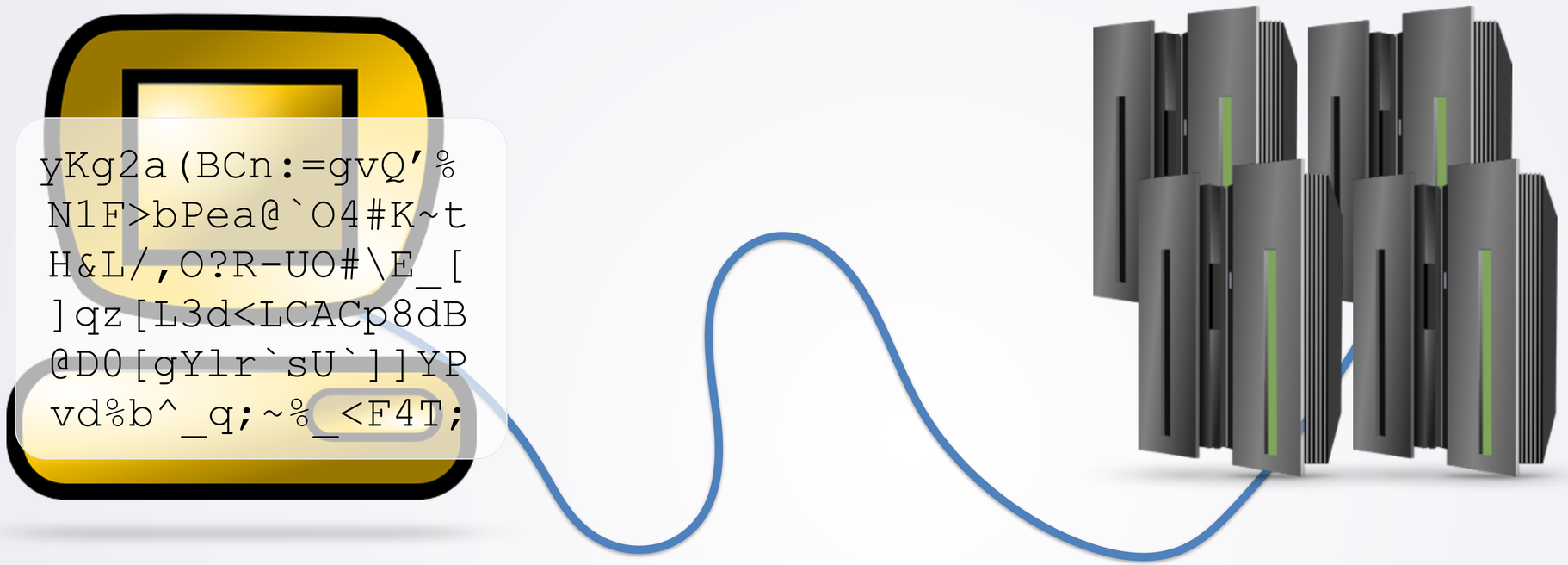
- You want to buy something online
  - Send credit card information to online store
- Do not want credit card info stolen
  - What makes it safe?

Online Shopping: Security



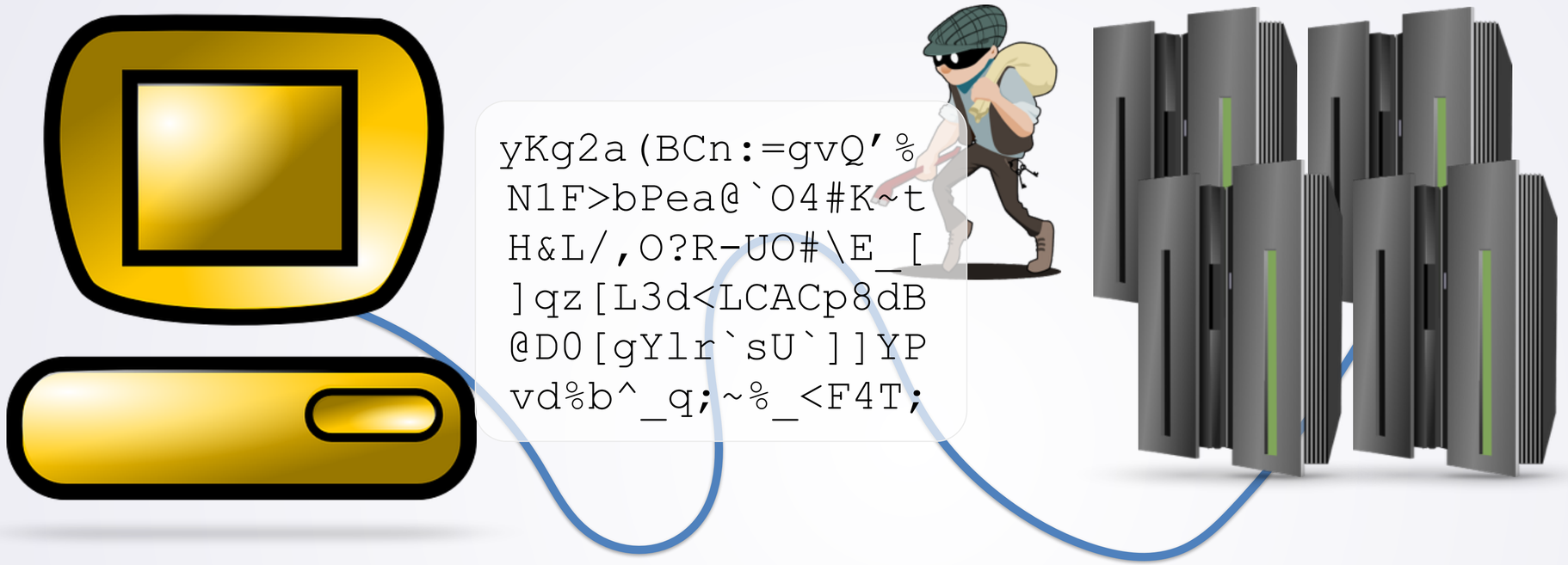
- Computer encrypts data before sending

Online Shopping: Security



- Computer encrypts data before sending

Online Shopping: Security



- Computer encrypts data before sending
- Thief can only see encrypted data
  - Very hard to decipher

Online Shopping: Security

- Computer encrypts data before sending
- Thief can only see encrypted data
  - Very hard to decipher
- Receiving server decrypts data

Modern Cryptography: https

The connection is encrypted and authenticated using AES_128_GCM and uses ECDHE_RSA as the key exchange mechanism.

$n = pq$

$\gcd(e, (p-1)(q-1)) = 1$

$c = m^e \pmod{n}$

$GF(2^8)$

- https = secure
- Uses modern cryptography: RSA + AES
- Math for those: a bit more than we'd like

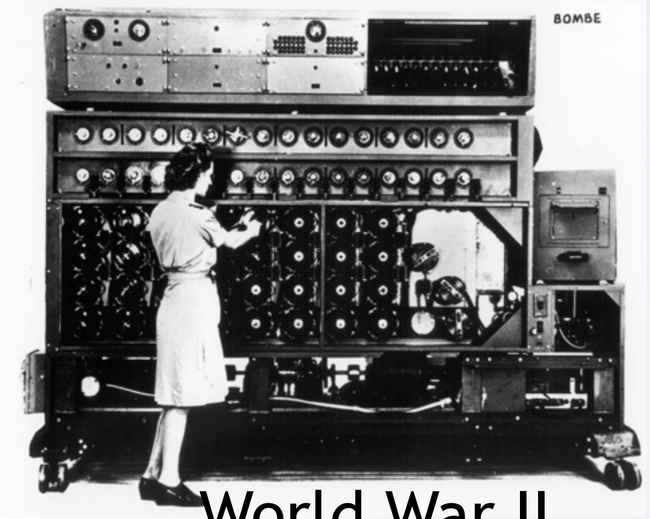
Ancient History to Modern Times

Mesopotamia
~1500 BCE

Egypt
~1900 BCE

Caesar Cipher

Roman Empire
~80 BCE



World War II

Vigenère Cipher
1553

https://

Present

- Modern cryptography: secure; advanced math
- Classical cryptography: insecure; simple math

Duke
UNIVERSITY

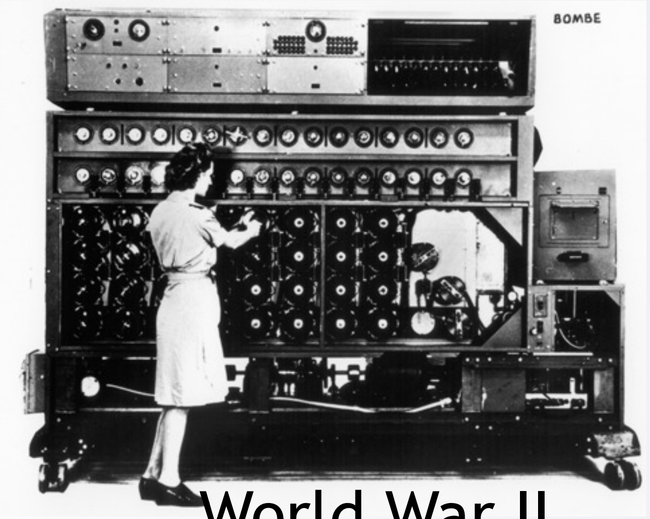
Ancient History to Modern Times

Mesopotamia
~1500 BCE

Egypt
~1900 BCE

Caesar Cipher

Roman Empire
~80 BCE



World War II

Vigenère Cipher
1553

https://

Present

- Modern cryptography: secure; advanced math
- Classical cryptography: insecure; simple math

Duke
UNIVERSITY