moz://a

Cryptography 101

Diane Hosfelt | @avadacatavra

July 8, 2017

What is cryptography?

Cryptography is a way to secure communications

- Secrecy
- Authentication

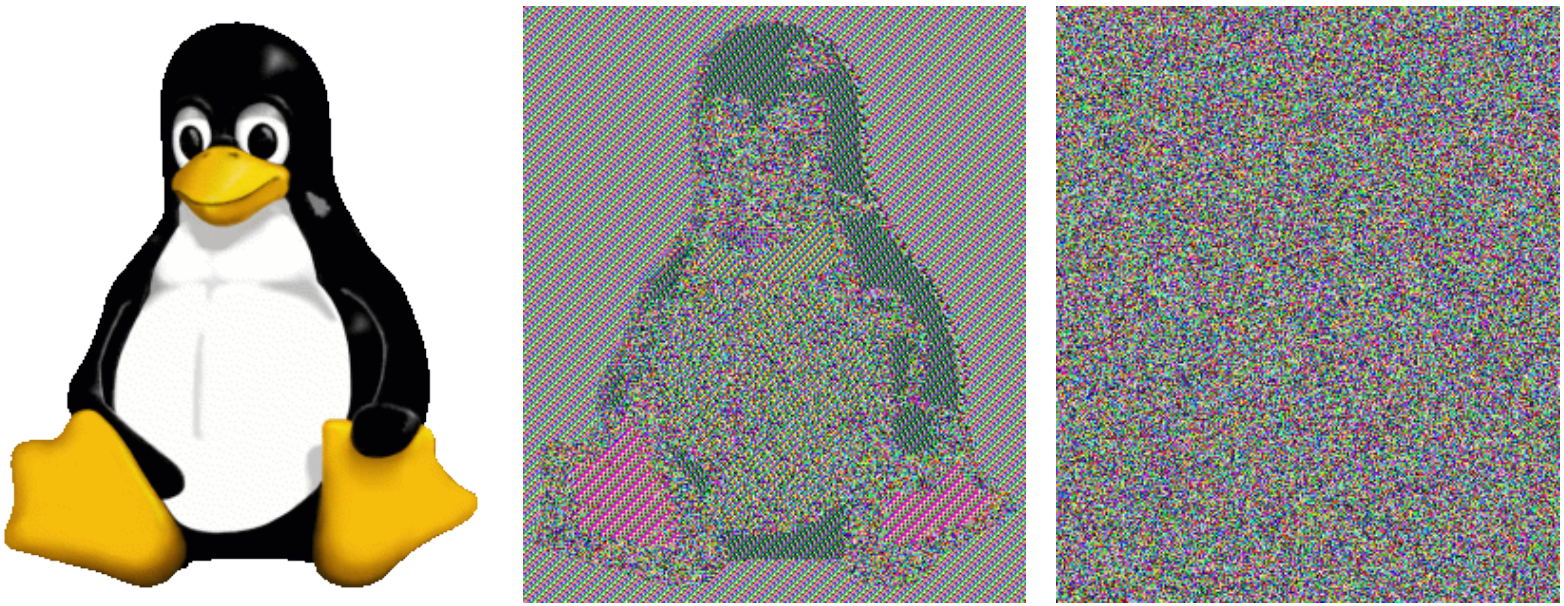


Figure 1: Try this! https://github.com/pakesson/diy-ecb-penguin

Classical vs. Modern Cryptography

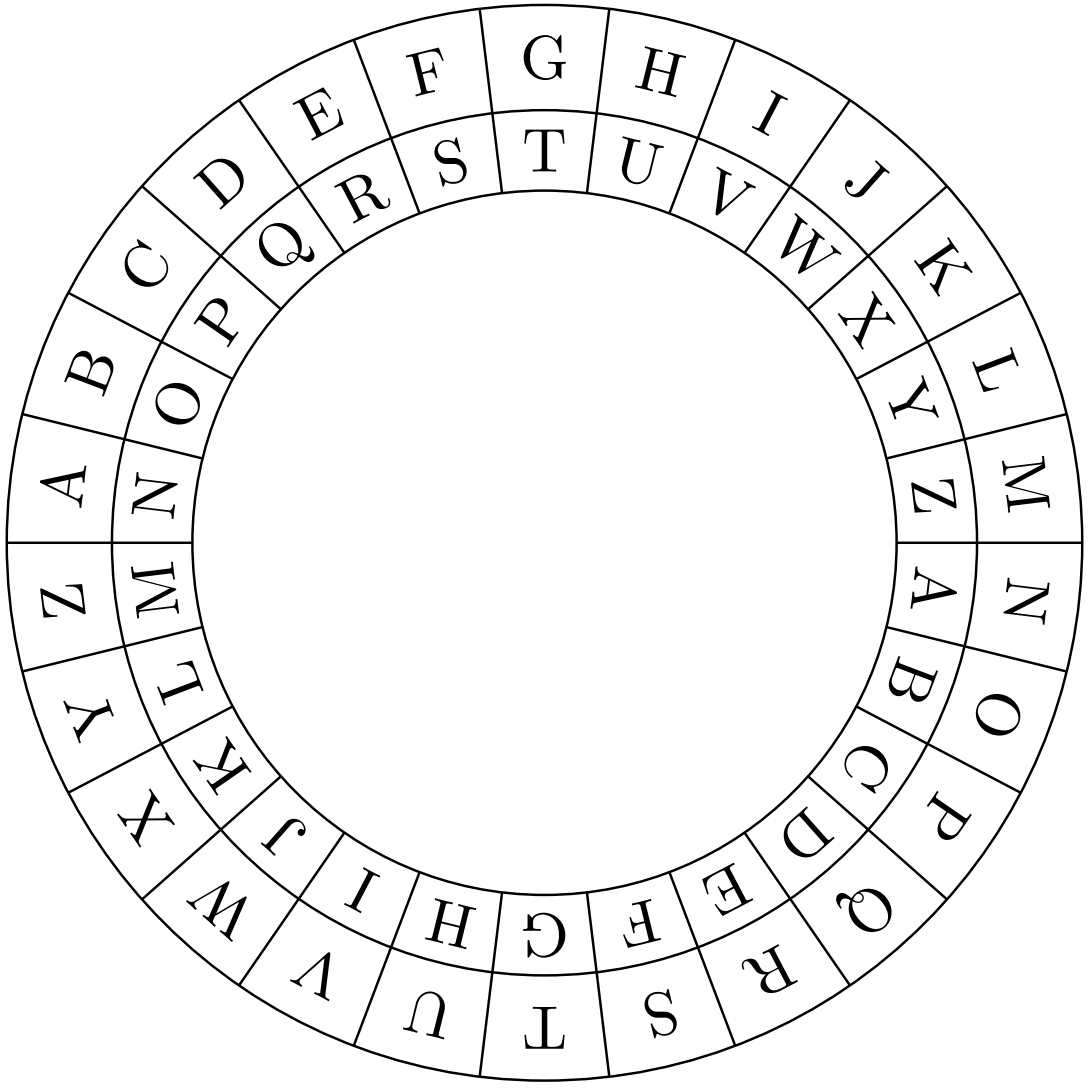
Classical:

- Security through obscurity
- Relied on secure channels for key exchange
- Substitution ciphers, codebooks

Modern:

- Kerckhoff's Principal
- Computers + Internet
- Public key cryptography allows insecure channels
- Encryption standards (DES, AES)

Caesar cipher



Caesar cipher

$$c = p + n \mod 26$$

$$p = c - n \mod 26$$

Why does this work?

Think of letters as numbers: a $= 0$, ..., z $= 25$

Try it out!

1. Choose a message to encrypt (the plaintext)
2. Choose a shift value (n)
3. For each letter in your plaintext, shift by *n*
    - If the shifted letter goes past 'z,' wrap around
4. Combine the shifted letters to get your ciphertext

Example

Plaintext Attack at dawn

Ciphertext Nggnpx ng qnja

Is this a good way to keep secrets?

- Brute force

Is there a way to improve this?

Figure 2: The Enigma machine, used by the Germans in WW2 to perform a complex polyalphabetic cipher

Is this a good way to keep secrets?

- Brute force
- Frequency analysis

Is there a way to improve this?

Figure 2: The Enigma machine, used by the Germans in WW2 to perform a complex polyalphabetic cipher

Is this a good way to keep secrets?

- Brute force
- Frequency analysis
- "Cribbing"

Is there a way to improve this?

Figure 2: The Enigma machine, used by the Germans in WW2 to perform a complex polyalphabetic cipher

Code

```
 2
 3 import string
 4 import sys
 5
 6 def caesar_shift(plaintext, shift):
 7     cipher = ""
 8     for char in plaintext:
 9         if char.isalpha():
10             # convert the character to a number
11             # 97 is the ascii number associated with a
12             # for modulo to work, we want the characters a-z to be from 0-25
13             # shift modulo 26, then reposition into the correct ascii location
14             shifted = (ord(char.lower()) - 97 + shift) % 26 + 97
15             cipher += chr(shifted)
16         else:
17             # if it's not alphabetic, just copy it
18             cipher += char
19     return cipher
20
21 def caesar_shift2(plaintext, shift):
22     alphabet = string.ascii_lowercase
23     shifted = alphabet[shift:] + alphabet[:shift]
24     table = str.maketrans(alphabet, shifted)
25     return plaintext.translate(table)
26
27 def main():
28     if len(sys.argv) < 3:
29         print("Please input shift and message")
30     shift = int(sys.argv[1])
31     message = sys.argv[2]
32     print(caesar_shift(message, shift))
33     print(caesar_shift2(message, shift))
34
35 if __name__ == "__main__":
36     main()
```

How has cryptography changed?

Kerckhoff's Principal

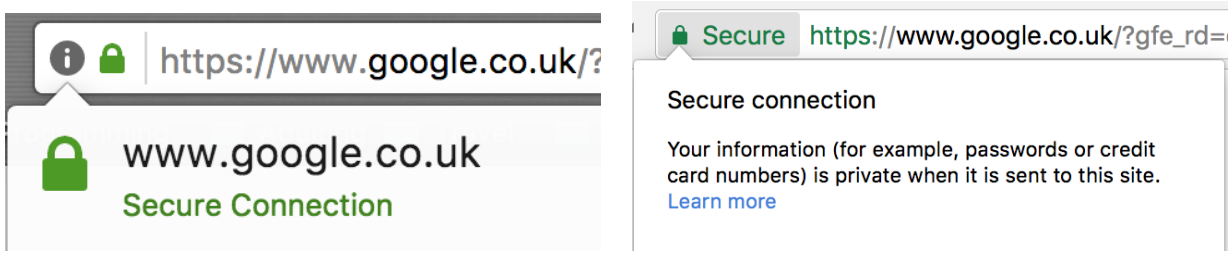
A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.

One time pad $\oplus$

- Vernam's cipher
- One-time pre-shared random key
- key length $\geq$ message length
- Perfect secrecy

Modern Crypto

Have you ever seen this when you're looking at a website?



- Transport Layer Security (HTTPS)
- Crypto currency (Bitcoin)
- Full disk encryption
- End-to-end encrypted messaging
- Hashing

Different types of cryptography

Symmetric Alice and Bob both know one secret key s_k

- What do you think is a problem with this method?

Asymmetric Two keys: one for encryption, one for decryption

- One way function

Example

Alice and Bob each have public and private keys, which they use to compute a shared secret key

- Diffie-Hellman exchange published in 1976
- RSA invented in 1978
- What ideas do you have about how they can make their secret key?

Public key cryptography

How can you pass a secure message to someone you've never met?

Public key cryptography!

- Instead of one key, have two
- Private key: only you know the private key
- Public key: anyone can see this

Public key Exchange

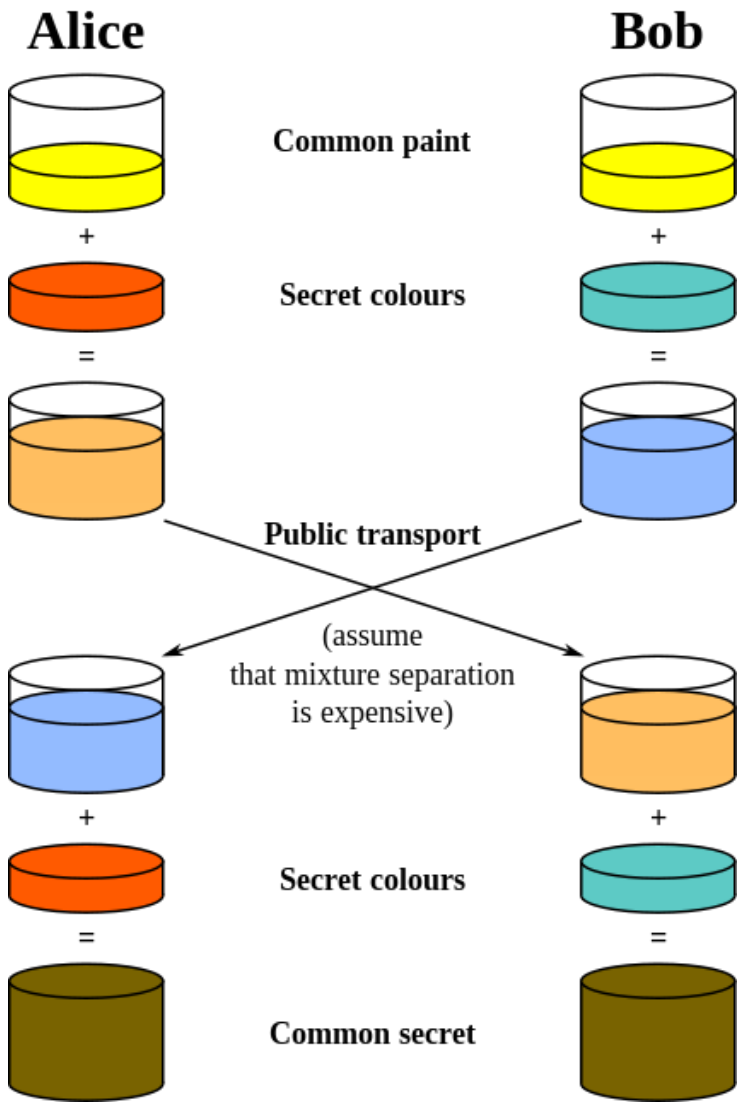
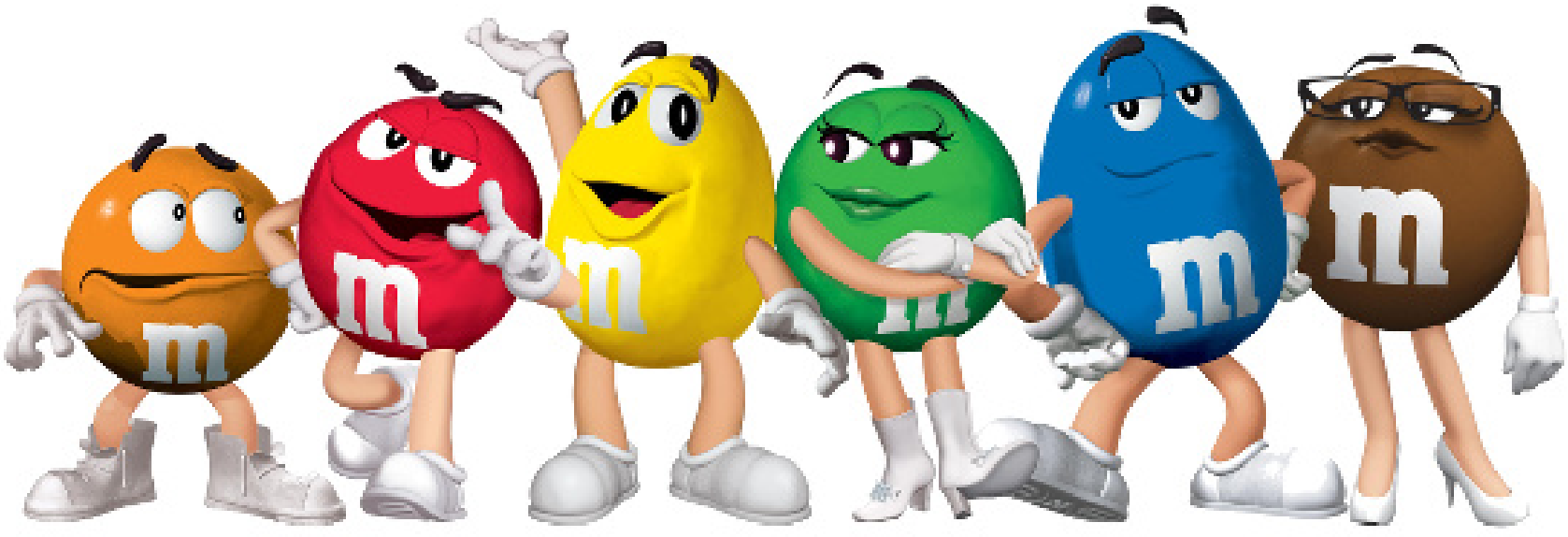


Figure 3: Image by A.J. Han Vinck, University of Duisburg

Chocolate Key Exchange



Questions?