Introduction

Michael Levin

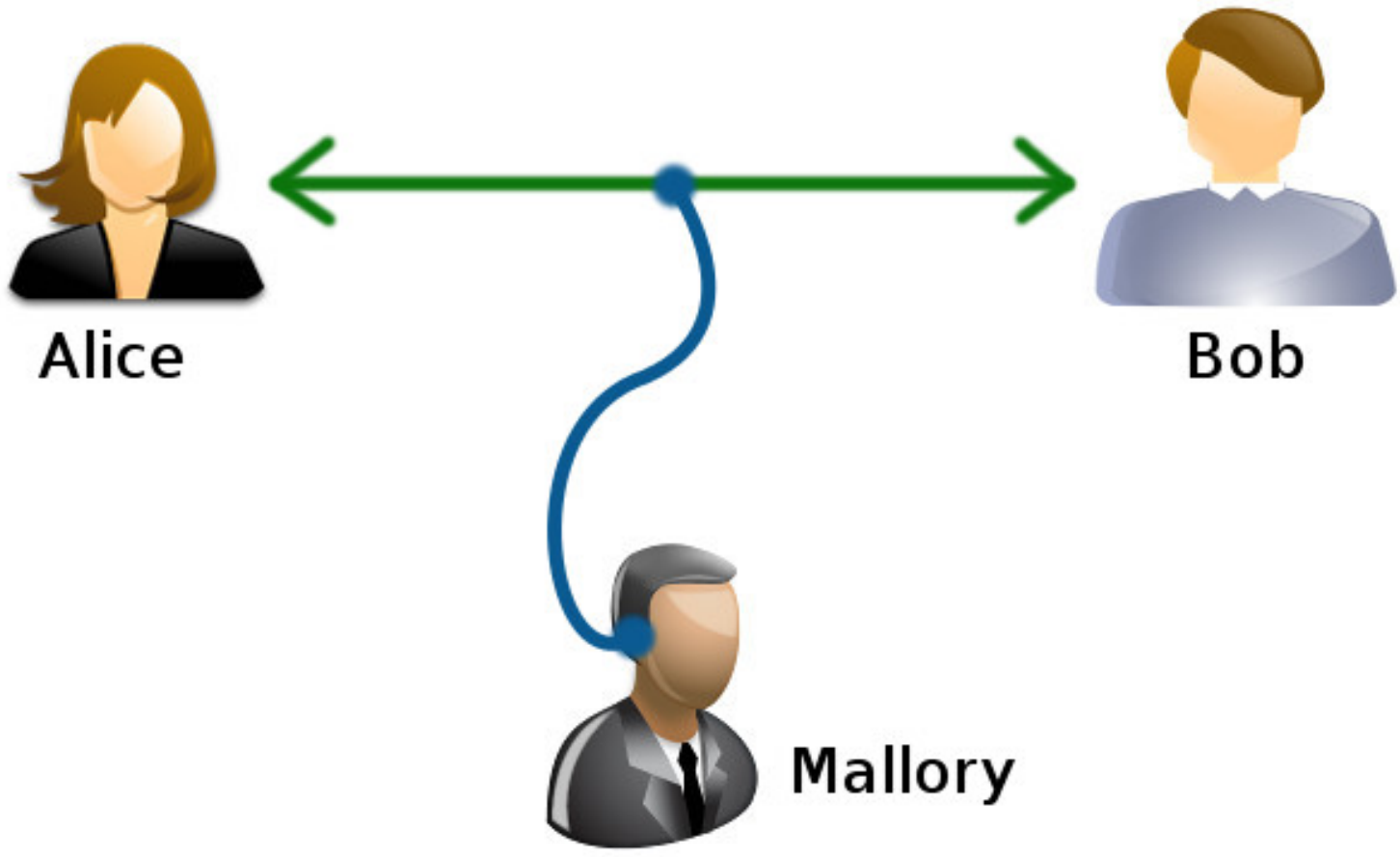
Computer Science Department, Higher School of Economics

Sharing Secrets

flickr.com

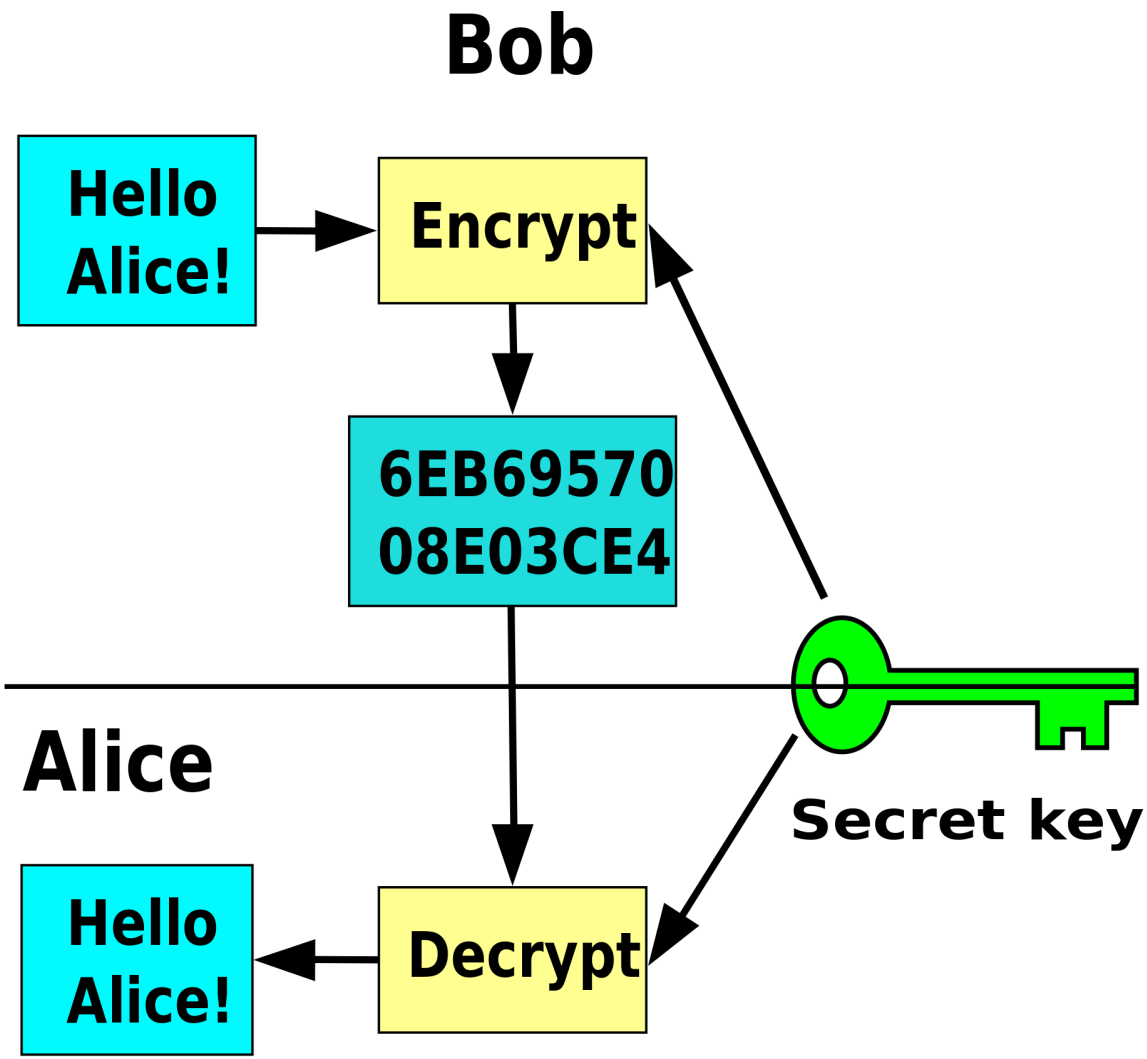
- Private communications via phone, e-mail, messengers
- Secure money transfer, online shopping
- Secure authorization for online services
- Secure software installation

Eavesdropping



wikipedia.org

Secret Code



wikipedia.org

Changing the Code

- If you use the same secret code many times, people around can guess what it is

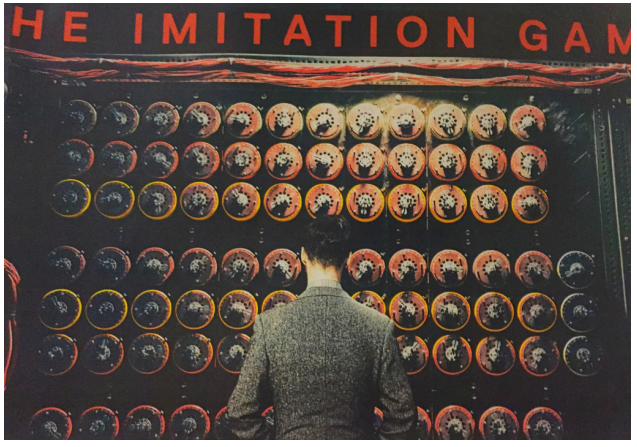
Changing the Code

- If you use the same secret code many times, people around can guess what it is
- Changing words to their opposites, replacing some words with other special words, rearranging letters — all these can be broken using statistics if there are many examples of encrypted messages

Changing the Code

- If you use the same secret code many times, people around can guess what it is
- Changing words to their opposites, replacing some words with other special words, rearranging letters — all these can be broken using statistics if there are many examples of encrypted messages
- Need to change the code often

- The Nazis changed their code once a day during the war, but the Allies led by Alan Turing still broke the cipher
- One should use different code for each communication

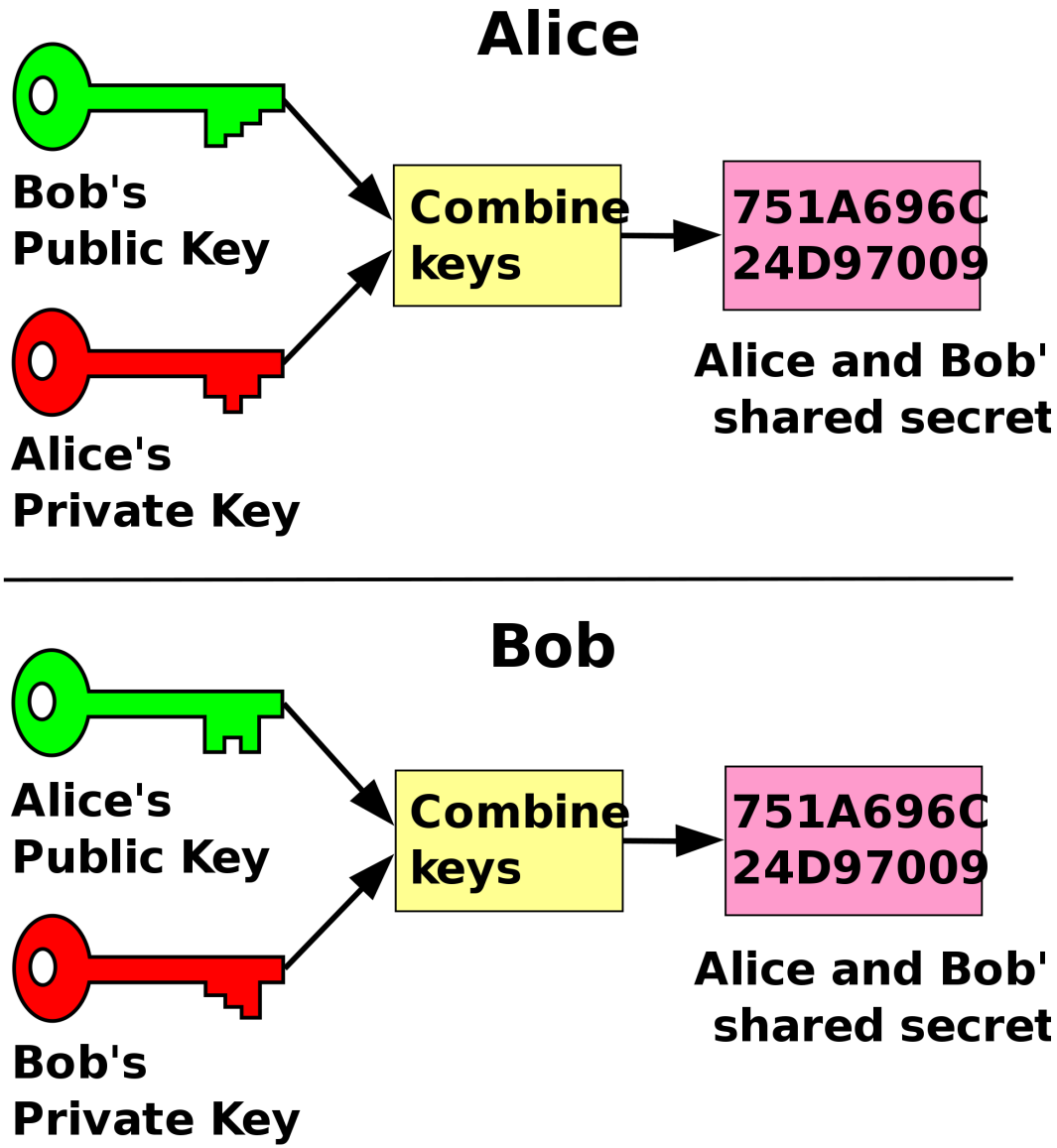


flickr.com

Sharing the Secret Code

- But how to share the secret code itself?
- Eavesdropper can get it
- What if you are communicating from different continents?
- And you need a new code for each communication

Public Key Cryptography



wikipedia.org

Cryptography

- Sharing secrets in such a way that noone can eavesdrop or change your messages
- Authorization and making sure a person cannot deny having sent the message
- Billions of money transactions use encryption everyday
- RSA encryption — arguably the most used program in the world
- This module — tools for cryptography
- Next module — keys and secure ciphers, how to break them if used incorrectly