First day: Basic ideas

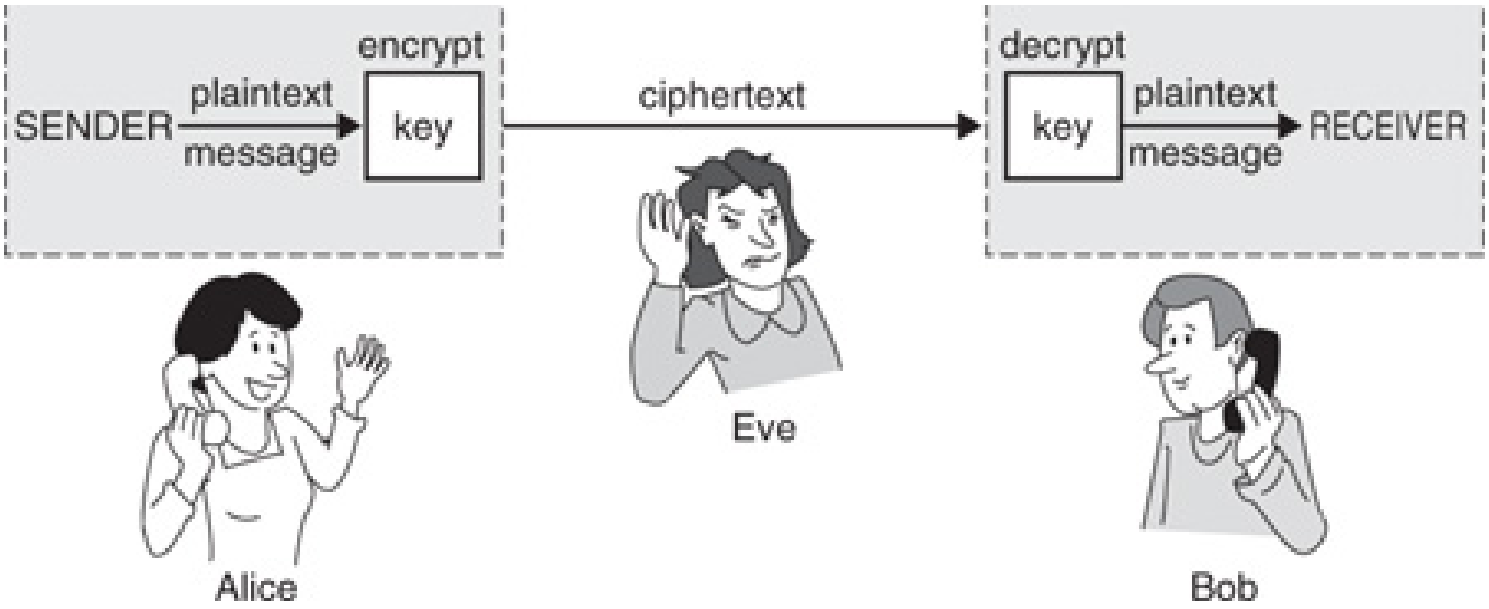
Christelle Vincent

University of Vermont

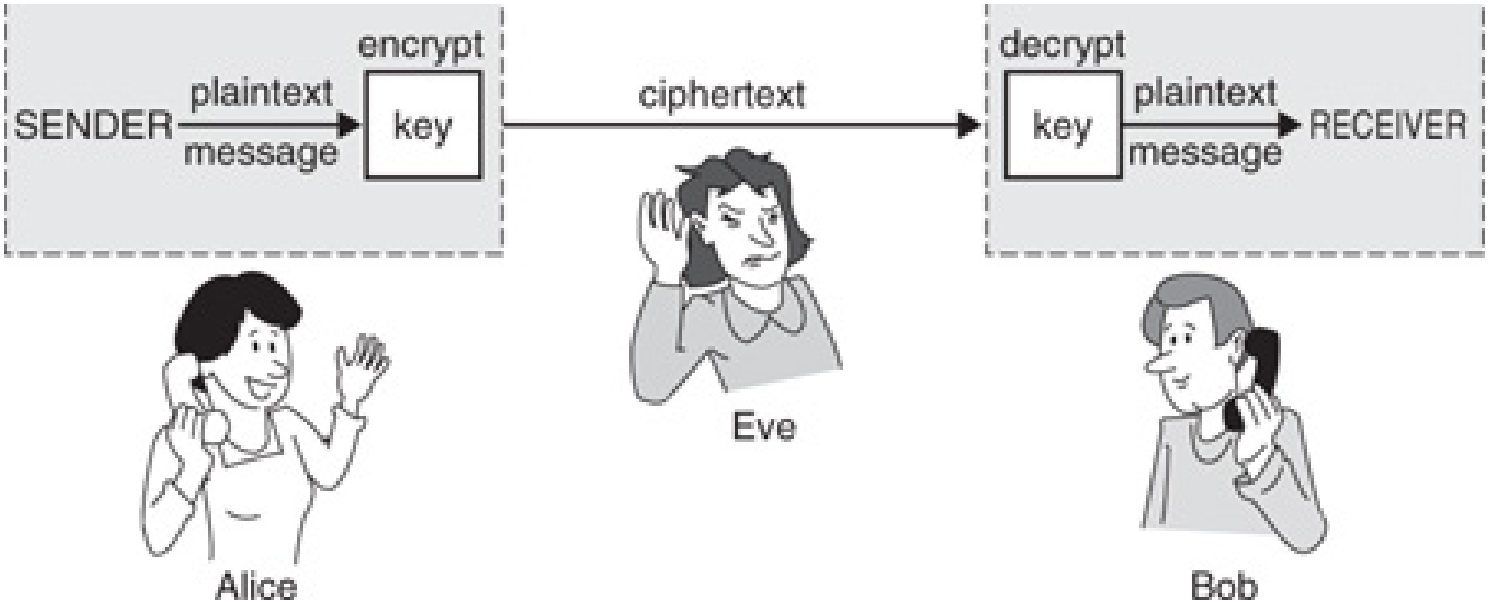
January 14, 2019

What is cryptography?

Cryptography is the practice and study of techniques for **secure communication in the presence of adverse third parties.**



Some vocabulary



Encryption refers to the process of changing ordinary text (*plaintext*) into unintelligible text (*ciphertext*).

Decryption is the reverse.

Keys in cryptography

A *cipher* is an algorithm used to encrypt and decrypt.

The operation of most good ciphers is controlled both by the algorithm and a parameter called a *key*.

Example: Caesar cipher

The algorithm of the Caesar cipher is to replace each letter by the kth letter preceding it in the alphabet.

The specific choice of k in a given instance of this cipher is the key.

To decrypt, use the **same** key k, but choose the kth letter following a given letter in the alphabet.

Cryptography then: Secret key cryptography

Main idea: Alice and Bob share **privately** the cipher and/or key they will use to communicate.

Examples:

- Caesar cipher ($\sim$100BC)
- Enigma machine (WWII)

Cryptography then: Secret key cryptography

This is also often called "symmetric key" cryptography, since Alice and Bob use the **same** secret key to encrypt and decrypt the message.

Drawback: Requires a secure exchange before setting up the secure exchange...

Cryptography now: Public key cryptography

In June 1976, Diffie and Hellman proposed the notion of *public key* or asymmetric key cryptography.[1]

In such a cryptosystem, Bob generates **two** sets of keys, one public and one private.

[1] Actually this was discovered in 1970 by Ellis at Government Communications Headquarters, but it was classified until 1997.

Cryptography now: Public key cryptography

Alice uses Bob's public key to encrypt a message to Bob,

and then Bob uses his private key to decrypt the message.

The simplifying assumption

Modern public-key cryptography is expensive computationally.

In reality it is used to encrypt a secret key, and then simpler, faster secret-key algorithms are used for communication.

Main idea

Public or asymmetric key cryptography relies on one thing:

There are some things in mathematics that are easy to do, but difficult to undo.

An example of a suitable problem

Which problem would you rather see appear on an exam:

1. Perform the multiplication 1489×701; or
2. Factor the number $1,043,789$.

Rough idea

Bob has the two primes 1489 and 701 as his private key, and the product $1,043,789$ as his public key.

He can publish his public key for everyone to see without fear that they can recover his private key, since factoring is difficult.[2]

[2] At least we think it is, if we don't have a quantum computer.

The RSA algorithm

This is the basis of the RSA algorithm, which is the first cipher we will study.

Published in 1978 by **R**ivest, **S**hamir and **A**dleman, it was the first civilian public key cryptography system.[3]

[3] Actually an equivalent system was developed by Cocks at GCHQ in 1973.