Cryptography and its relevance in today's world

Fighting back against global surveillance

1. Relevance of cryptography
   - NSA revelations
   - Why you should care
2. Goals and principles of cryptography
   - Goals
     - Confidentiality
     - Authentication and integrity
   - First example
   - Principles
     - What is required for a cryptosystem
     - Algorithmic complexity
     - Symmetric cryptography
     - Asymmetric cryptography
3. Practical usage
   - Free software
   - Using encryption

Quote of Wendell Phillips

Eternal vigilance is the price of liberty; power is ever stealing from the many to the few. *The manna of popular liberty must be gathered each day or it is rotten. The living sap of today outgrows the dead rind of yesterday. The hand entrusted with power becomes, either form human depravity or esprit de corps, the necessary enemy of the people. Only by continued oversight can the democrat in office be prevented from hardening into a despot; only by unintermitted agitation can a people be sufficiently awake to principle* ***not to let liberty be smothered in material prosperity.***

What we currently know about what the NSA is doing

- The NSA is eavesdropping [a] on every major US company's traffic (often with their cooperation), that is to mean Google, Yahoo, Facebook, Microsoft, Apple and so on.

a. eavesdrop : to listen secretly to a private conversation

What we currently know about what the NSA is doing

- The NSA is eavesdropping [a] on every major US company's traffic (often with their cooperation), that is to mean Google, Yahoo, Facebook, Microsoft, Apple and so on.
- The NSA is intercepting every bit of what is going through the submarine cables, analyzing it, and storing meta-datas.

a. eavesdrop : to listen secretly to a private conversation

What we currently know about what the NSA is doing

- The NSA is eavesdropping [a] on every major US company's traffic (often with their cooperation), that is to mean Google, Yahoo, Facebook, Microsoft, Apple and so on.
- The NSA is intercepting every bit of what is going through the submarine cables, analyzing it, and storing meta-datas.
- Almost all phone calls around the world are intercepted. (Echelon program).

a. eavesdrop : to listen secretly to a private conversation

Any time that you're developing a new product, you will be working closely with the NSA.

Ira Rubenstein, Microsoft attorney, 1998 to CNN

NSA systematically intercepts international communications, both voice and cable.

General Allen, Director of the NSA testifying before Congress in 1975

So how are those surveillance powers checked ?

- By secret courts
- operating according to secret regulations
- issuing global warrants
- secret rules that President Obama isn't even willing to share with Congress Intelligence Committee.

Good news, all major countries do the same spying at their level.

But why should you care about any of this?

- You care about privacy.

But why should you care about any of this ?

- You care about privacy.
- You think people in power should respect the law/constitution and are accountable of their acts.

But why should you care about any of this ?

- You care about privacy.
- You think people in power should respect the law/constitution and are accountable of their acts.
- Economic impact (theft of technology and so on).

But why should you care about any of this ?

- You care about privacy.
- You think people in power should respect the law/constitution and are accountable of their acts.
- Economic impact (theft of technology and so on).
- You own/carry important datas and you want to protect them.

But why should you care about any of this ?

- You care about privacy.
- You think people in power should respect the law/constitution and are accountable of their acts.
- Economic impact (theft of technology and so on).
- You own/carry important datas and you want to protect them.
- You are going to the US : be careful, it is estimated that more than 100, 000 people are working for the NSA (see [?], some NSA employees spied on their (ex-)boyfriends/girlfirends)

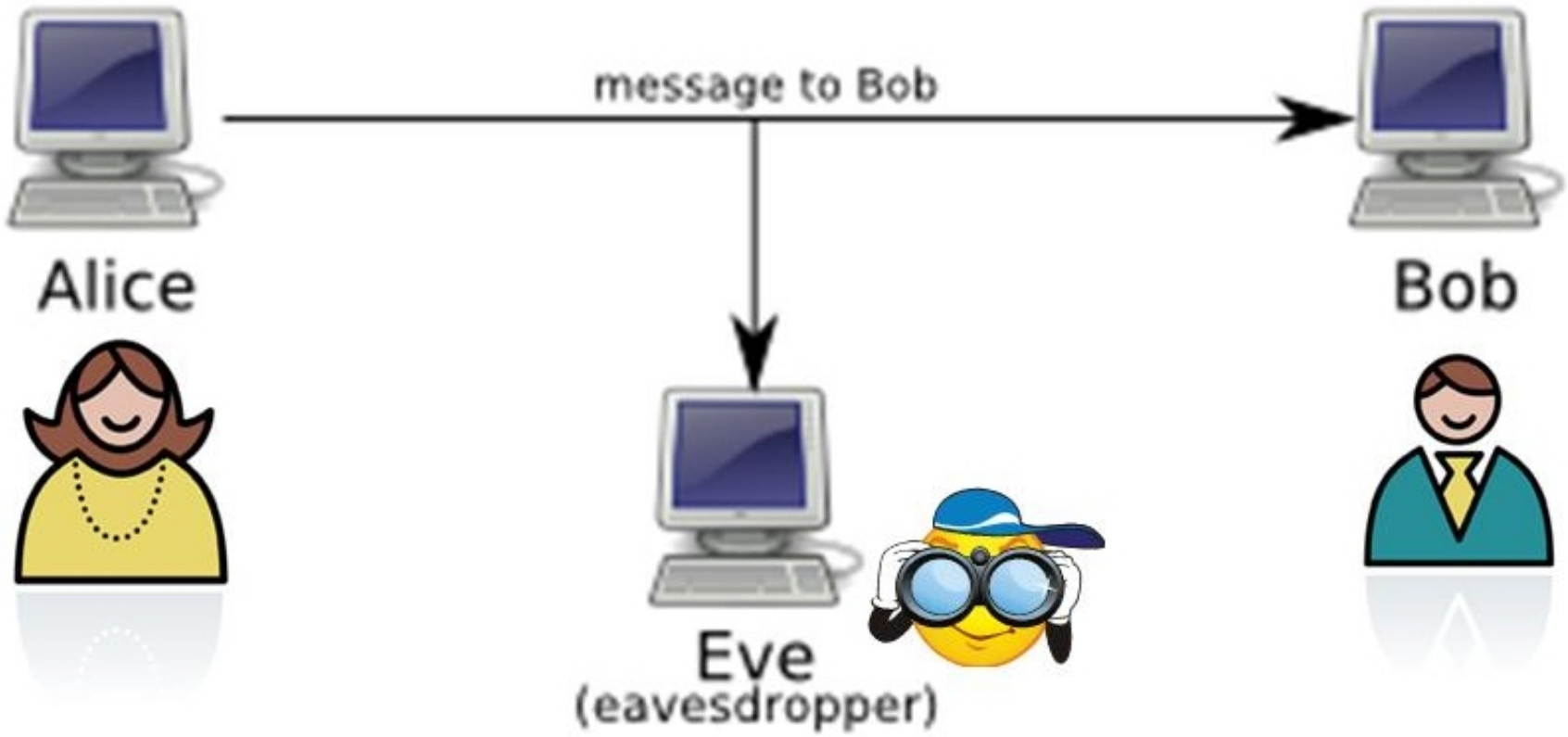
But why should you care about any of this ?

- You care about privacy.
- You think people in power should respect the law/constitution and are accountable of their acts.
- Economic impact (theft of technology and so on).
- You own/carry important datas and you want to protect them.
- You are going to the US : be careful, it is estimated that more than 100, 000 people are working for the NSA (see [?], some NSA employees spied on their (ex-)boyfriends/girlfirends)
- You are going to a country with more restrictive laws on freedom of speech and with extensive regulation of Internet.

It is insufficient to protect ourselves with laws ; we need to protect ourselves with mathematics.

Bruce Schneier, cryptographer

Good news : You can protect yourself by using cryptography. The main current algorithms are not known to have any serious weakness.



Problem of confidentiality

A message M (plain text) has to be transmitted on a canal, but it could be intercepted.

The aim of cryptography is to prevent the attacker to be able to understand the message, or to exploit it in any way.

Problem of authentication and integrity

1. authentication [a] : the message M is coming from the right person
2. integrity : M hasn't be modified in any way.

a. authenticate : To establish the authenticity of ; prove genuine

When you connect to your bank, you wan't to be sure that it is really your bank you are connecting to, and you want to be sure the right amounts are transferred.

Caesar cipher

Pick a number n between 0 and 25 and then replace all letters of the message by the n-th letter after them (restarting at A if necessary).

For example $M = B$ with $n = 3$ becomes E.
$M = OUI$ with $n = 10$ becomes YES.

n is called the *key* of the cipher. It is a parameter in the encryption.

The number of possible keys is called the *keysize*.

Kerckhoffs's principle

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

Bad example : Enigma machines used by the Germans during World War 2

You can't be sure of a non published algorithm.
It is far more complicated to guess a random number (the key) than to find how a secret algorithm works.

Absolutely secure vs Computationally secure

- absolutely secure : it is impossible to retrieve the plaintext without knowing the key.
- computationally secure : retrieving the plaintext without knowing the key won't be possible with many computational power before a long period of time

> *If all the personal computers in the world - 260 million computers - were put to work on a single PGP-encrypted message, it would still take an estimated 12 million times the age of the universe, on average, to break a single message.*

William Crowell, Deputy Director of the National Security Agency, March 1997

What is complexity ?

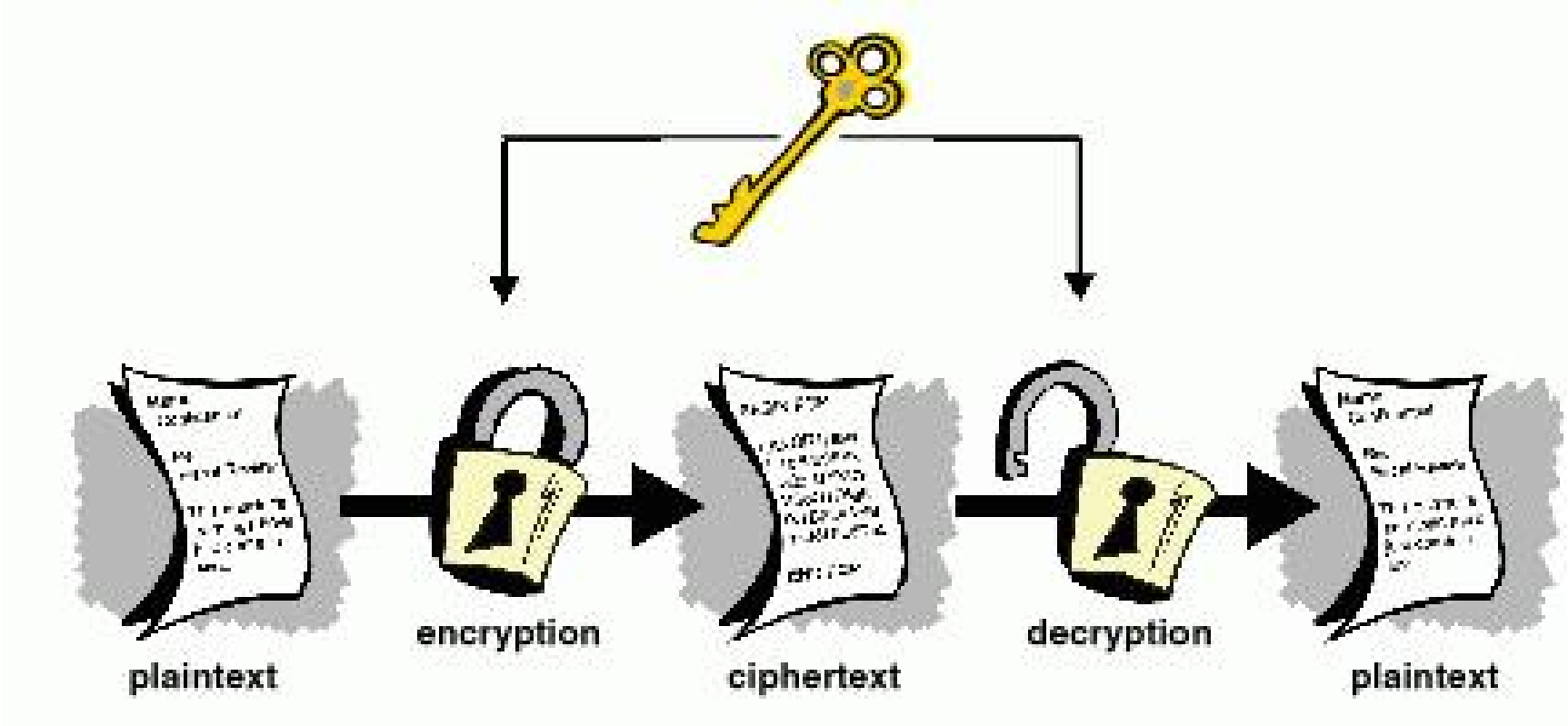
Problems in computer sciences can be very easy or very hard :
Easy problems : adding two integers, multiply two integers, finding the shortest path on a map between two points
Hard problems : factoring integers, discrete logarithms

One measures complexity in number of elementary operations.

- Adding two n-bits integers is $O(n)$. Multiplying them is $O(n^2)$ and even $O(n \log n \log \log n)$.
- Factoring a random integer is $O(2^{n/2})$ or a bit better.

Trapdoor function : easy to compute the inverse if you know the secret. Very hard if you don't know it.

A symmetric algorithm uses one key for both encryption and decryption. It is analogous to putting the message in a locked stash.
The advantages : very fast encryption and decryption



Main problem : how do you communicate the secret key ?

Diffie–Hellman key exchange : an example of how you can safely exchange a key

1. Both nodes agree on two values (g and n)

2. Generate a random value (x)

3. $A = G^x \bmod n$

2. Generate a random value (y)

3. $B = G^y \bmod n$

4. A and B Values are exchanged

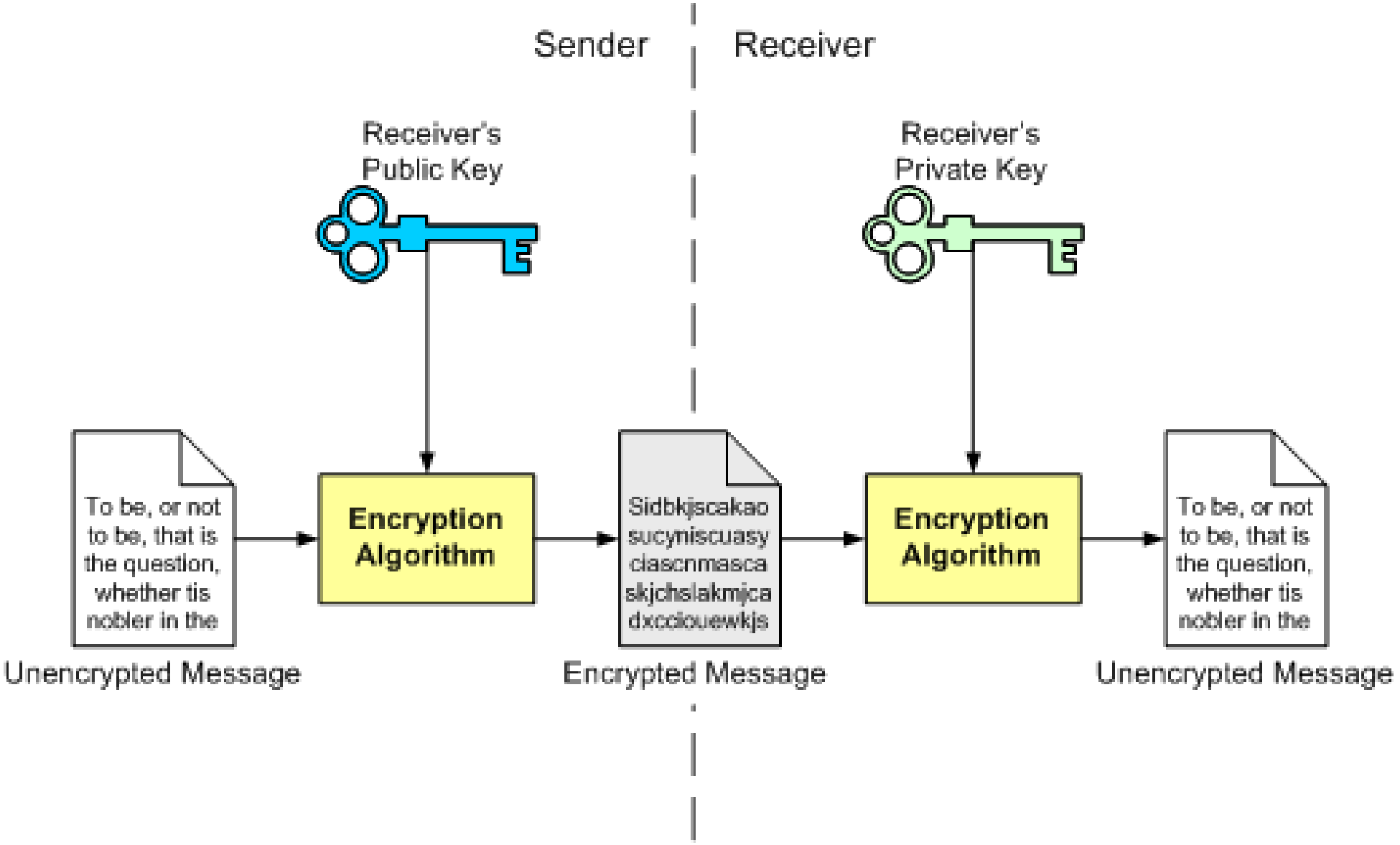
5. $K1 = B^x \bmod n$

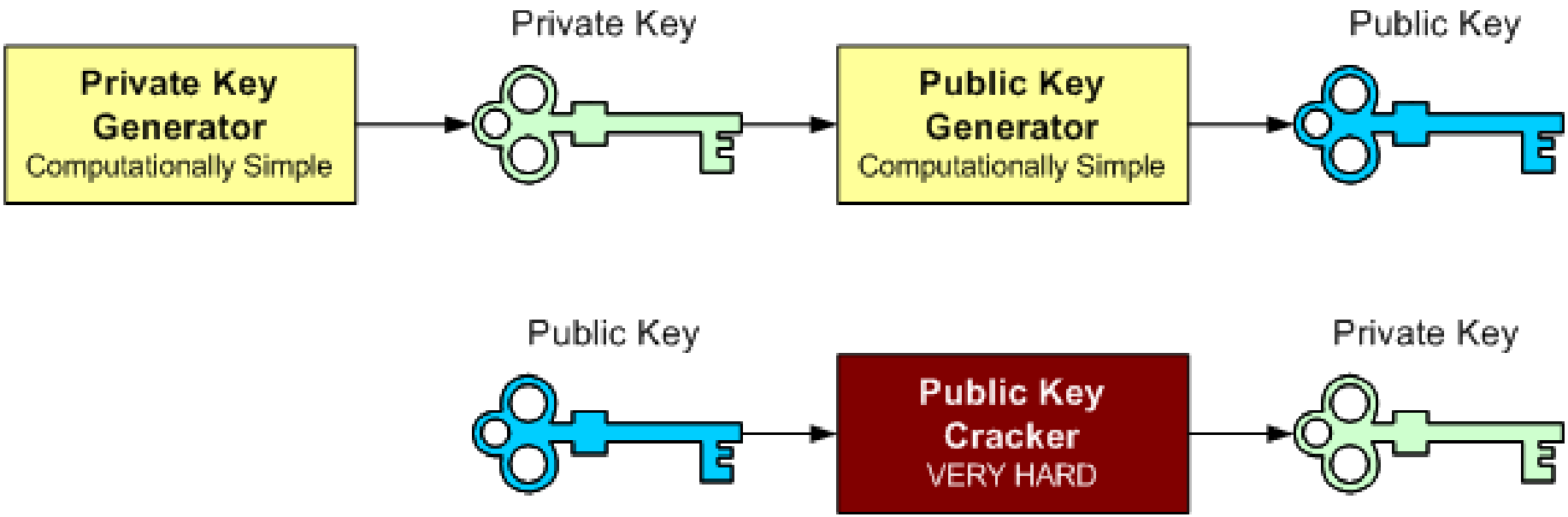
5. $K2 = A^y \bmod n$

$K1$ and $K2$ should be the same and are the secret key

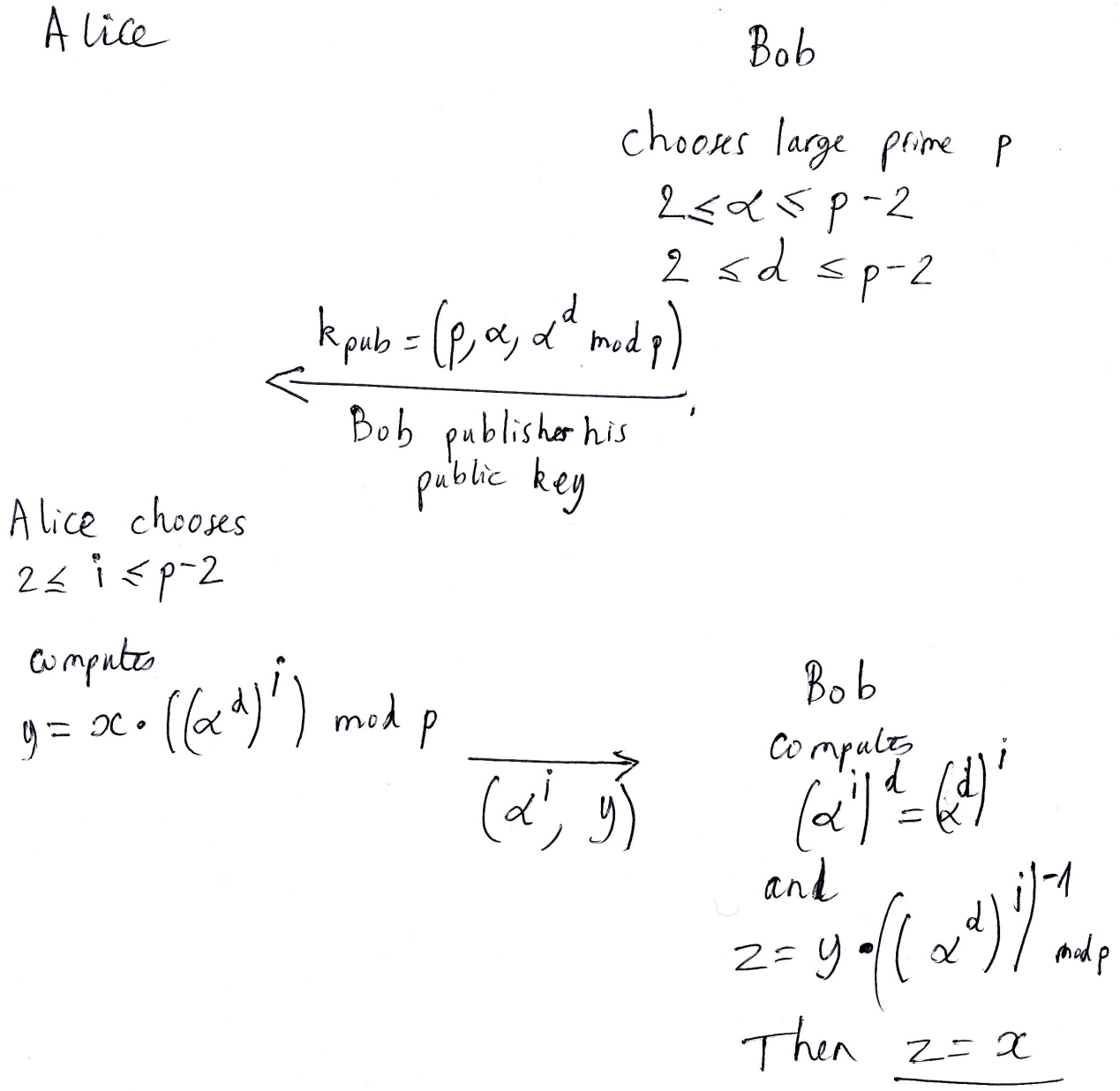
Public key cryptosystem

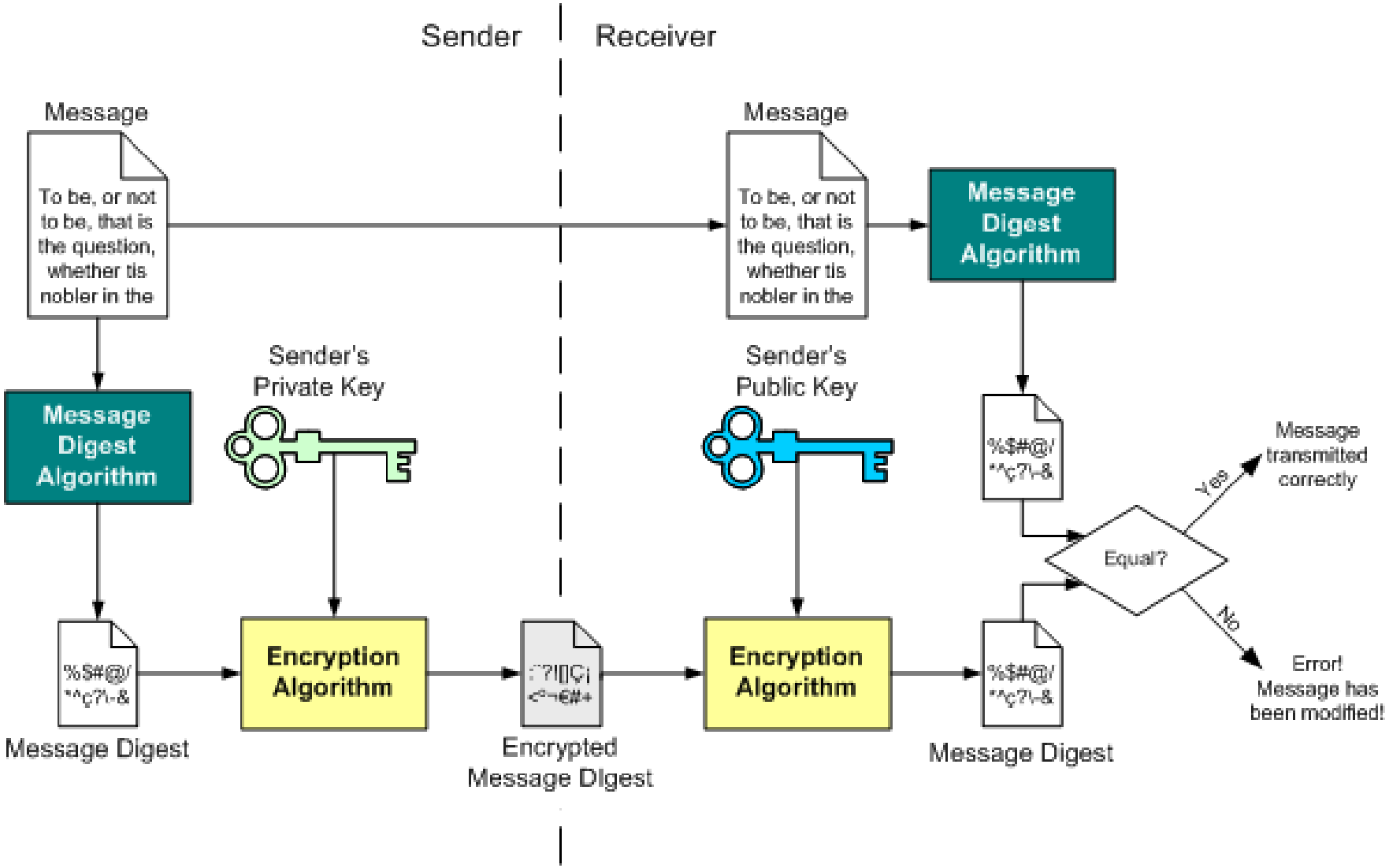
For such systems, there are two keys : one for encrypting, one for decrypting.




Private Key Generator
Computationally Simple
Private Key
Public Key Generator
Computationally Simple
Public Key
Public Key
Public Key Cracker
VERY HARD
Private Key

Completing a public key cryptosystem with the precedent example :




Sender
Receiver
Message
To be, or not to be, that is the question, whether tis nobler in the
Message
To be, or not to be, that is the question, whether tis nobler in the
Message Digest Algorithm
Sender's Private Key
Sender's Public Key
Message Digest Algorithm
%$#@/ *^ç?\-&
%$#@/ *^ç?\-&
Encryption Algorithm
Encryption Algorithm
%$#@/ *^ç?\-&
Equal?
Yes
Message transmitted correctly
No
Error! Message has been modified!
Message Digest
Encrypted Message DIgest
Message Digest

On the importance of open source

- Free software : the recipe or the code is public.
- You shouldn't ever trust closed source softwares. They offer you no guarantee on what is happening when they are working.
  US companies are putting backdoors in their softwares upon request by the NSA. (This isn't conspiracy theory, see [?], [?] and [?])

A few practical advices

- HTTPS : it is HTTP with encryption (public key algorithm)
  Use HTTPS everywhere plugin with your browser.
- Use PGP (pretty good privacy) for your emails whenever it is possible.
  (Download Thunderbird and Enigmail plugin).
- Encrypt your laptop's hard drive (or at least important files)
- For more information (phone encryption and so on), go to `https://prism-break.org`.

How much do you care about privacy?
Would you use cryptography?