Cryptography basics

By a noob, for the noobs

Alexandre Aubin
HackStub
July 10th, 2013

Outline

Why ?

Symmetric cryptography

Asymmetric cryptography

Off-the-record (OTR) messaging

Stuff to play with

Disclaimer

- Lolcats for the lulz.

- I am not an expert.
- This is the basic stuff.

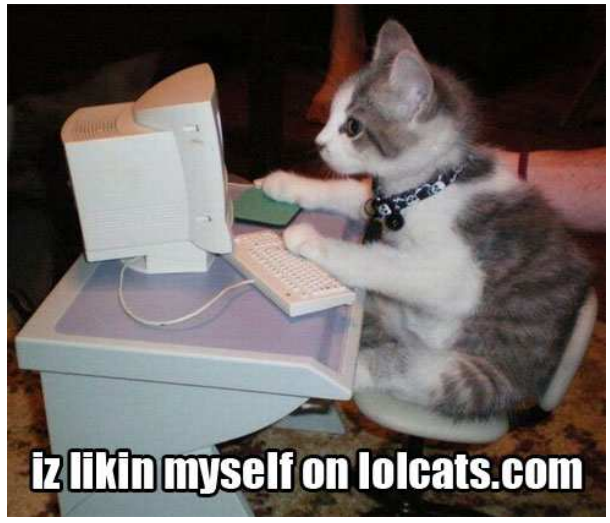
Why ?

Context

- Arab spring
- PRISM / mass surveillance

Goal : cryptography should become an easy-to-use tool

- 1) Theory (today)
- 2) Practice (later (or today))



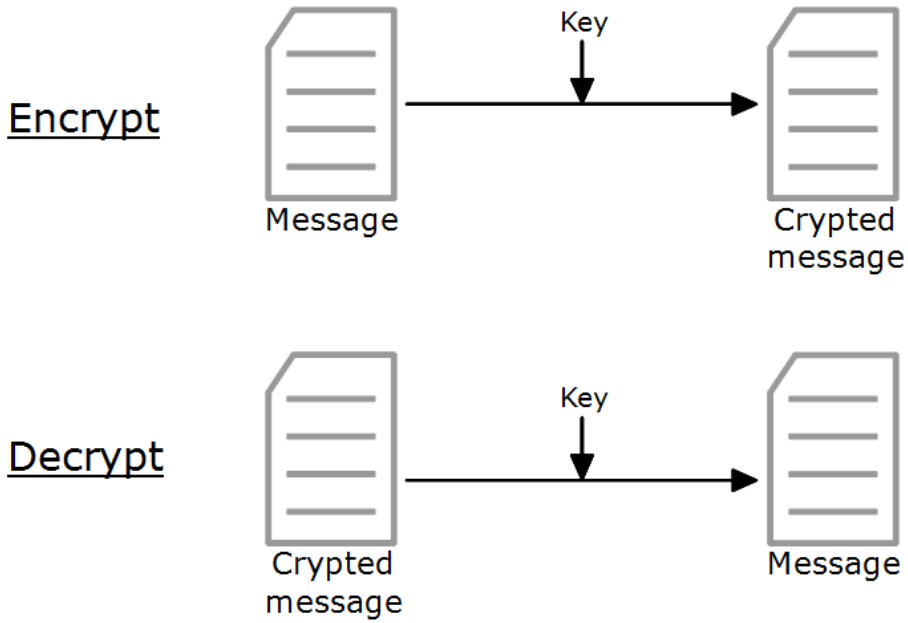
Basic example

Text : « when does the narwhal bacon ? »
Example 1 : « xifo epft uif obsxibm cbepo ? »
Example 2 : « 23080514 04150519 200805 14011823080112 0201031514 ? »

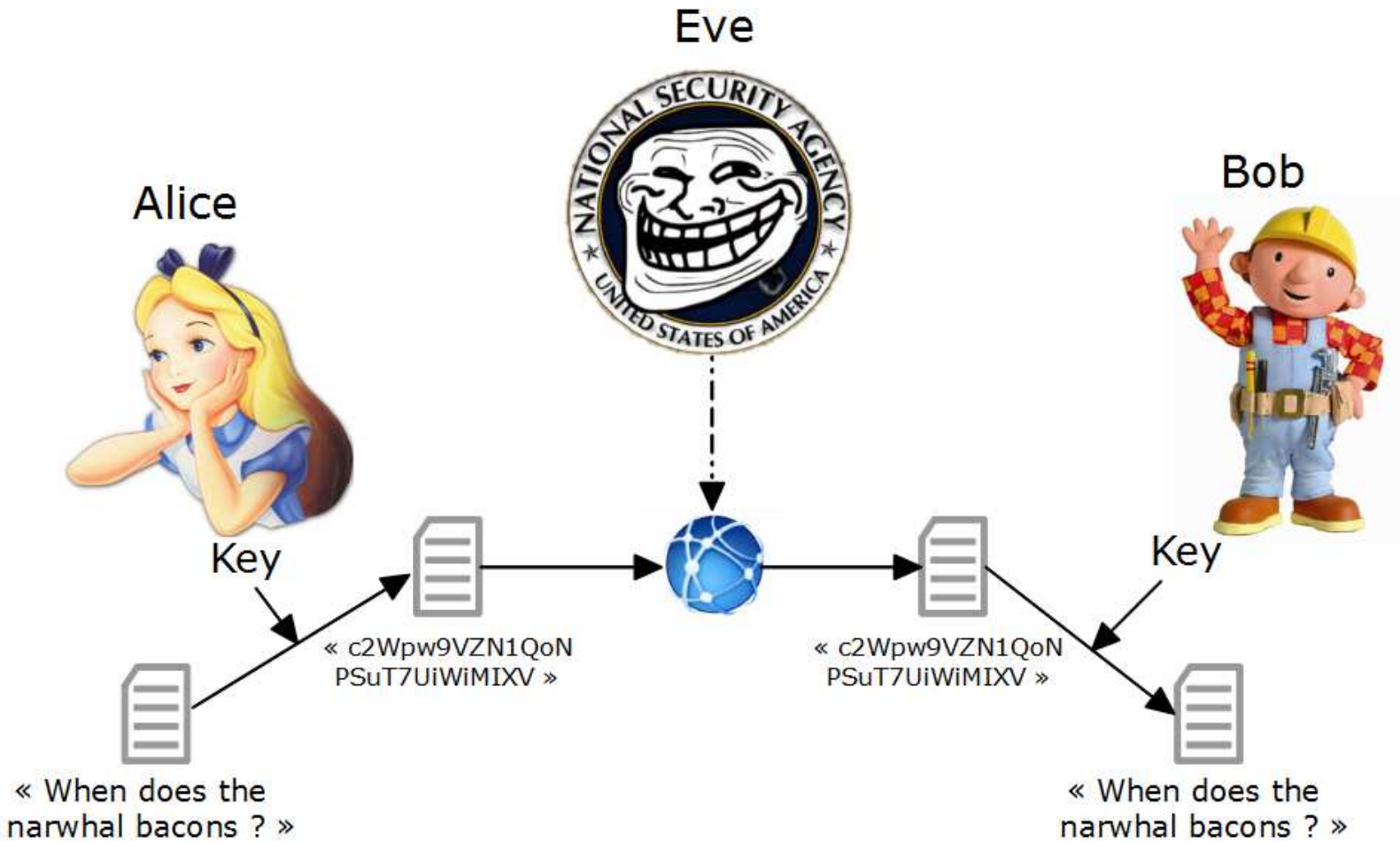
to encrypt = to transform an information into something not understandable without the relevant key

Symmetric cryptography

- **One shared key** used for both encryption and decryption.
- The problem : this key have to be transmitted, but kept secret.

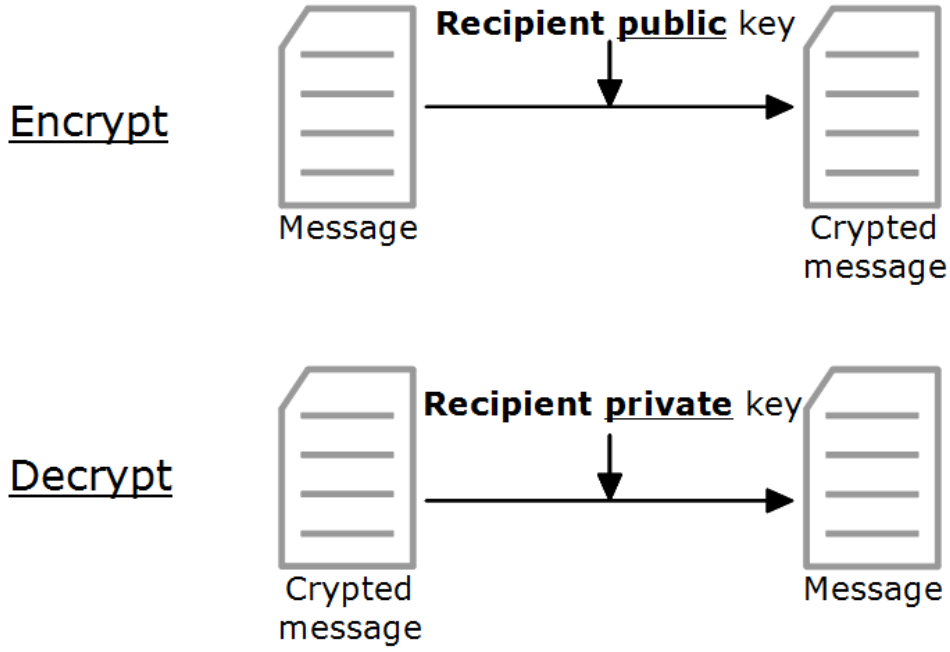


Symmetric cryptography

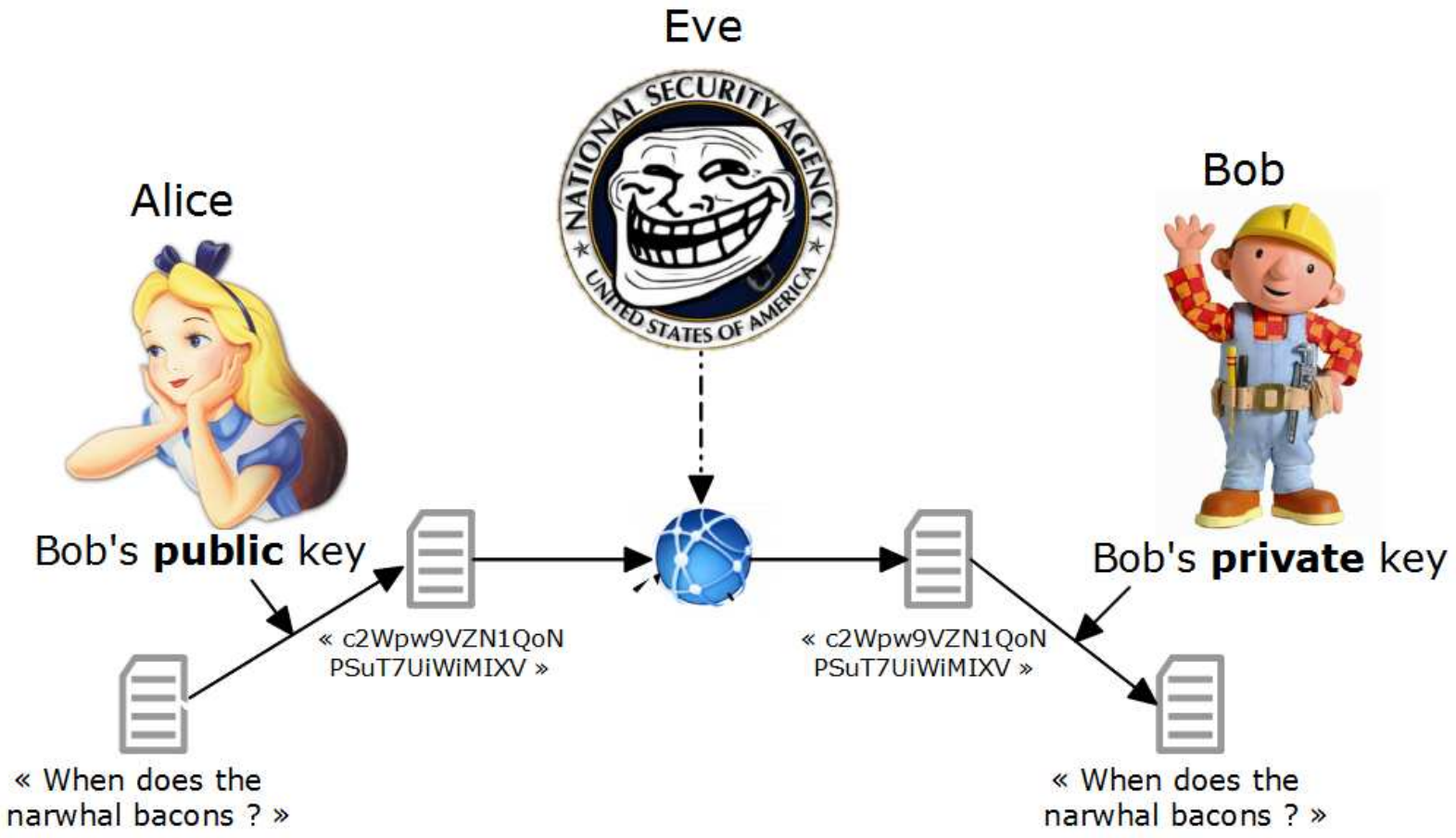


Asymmetric cryptography

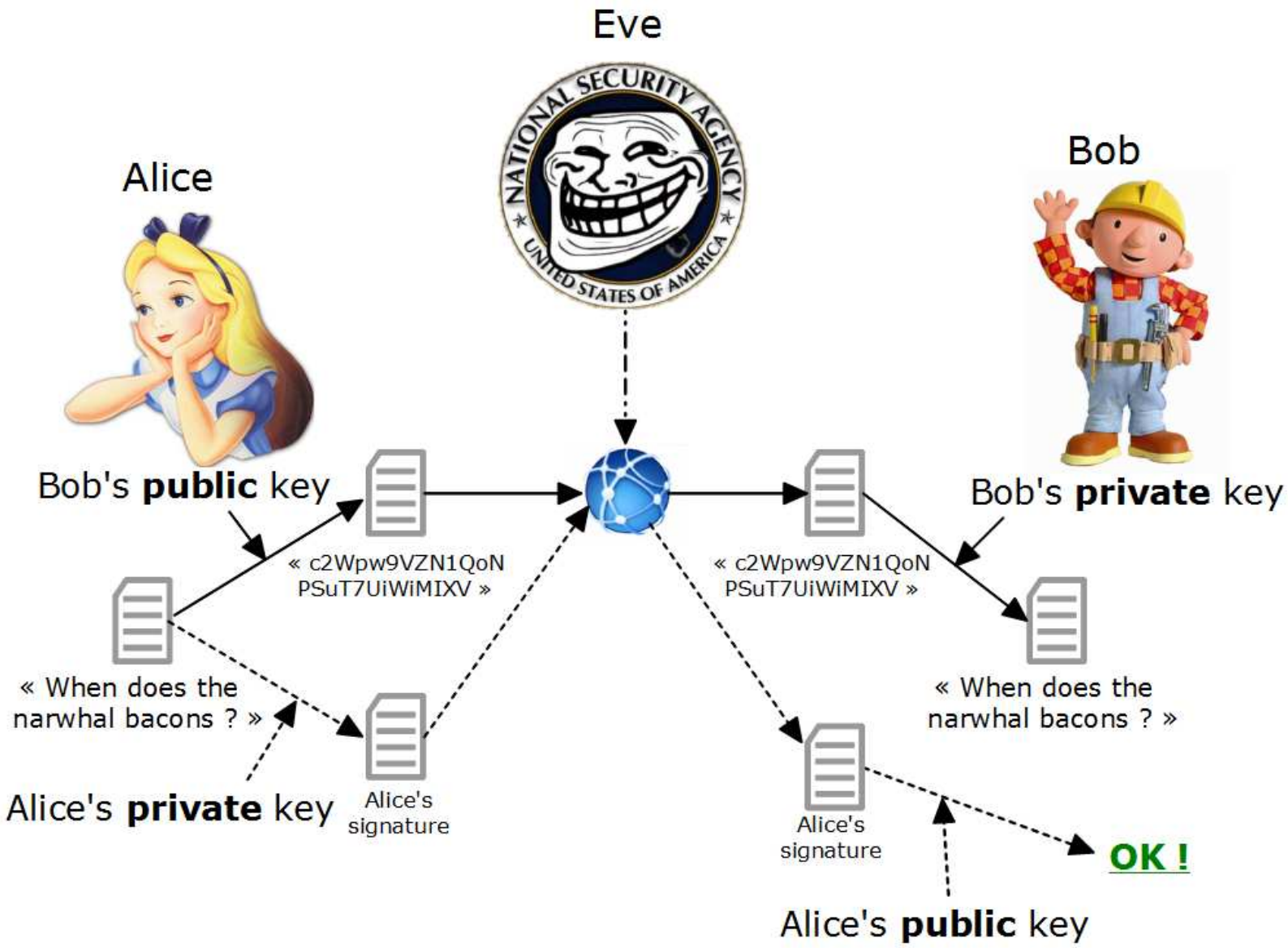
- Each user has **a pair** of cryptographic keys : (**private** key, **public** key)
- The **public** key is used to encrypt messages.
- Only the **private** can decrypt the encrypted messages.
- The **private** key is not deducible from the **public** key.
- (The cryptographic algorithm and key generation is a complex math thing)



Asymmetric cryptography



Asymmetric cryptography



Asymmetric cryptography

- Encryption
- Authentication
- Integrity

Off-the-record (OTR) messaging

OTR is used for (mainly ?) for secure Instant Messaging

Allows :

- Encryption (secure exchange of per-session symmetric keys)
- Authentication (using asymmetric keys)
- Perfect foward secrecy (private keys compromisation does not compromise previous conversations)
- Deniability

Stuff to play with

- Mail : PGP/GPG, Bitmessage
- Chat : OTR (over xchat, cryptocat, xmpp, ..)
- Web : SSL certificates, SSH tunnels
- Stockage : TrueCrypt
- Money : Bitcoin
- ???

Stuff to play with

Lurk moar

Cryptographie et sécurité / Skhaen PSES 2012
cyphercat.eu

Telecomix crypto-munitions
Firefox extensions for the crypto-anarchist

PGP (on Wikipedia)
Public key certificate (on Wikipedia)

OTR messaging protocol description
Moar stuff on OTR (cypherpunks.caotr)


Brain Download:
iz compltes.
ICANHASCHEEZBURGER.COM