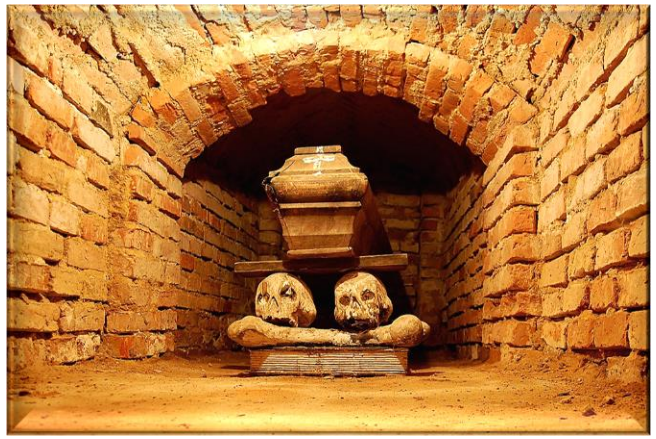
La sécurité prouvable

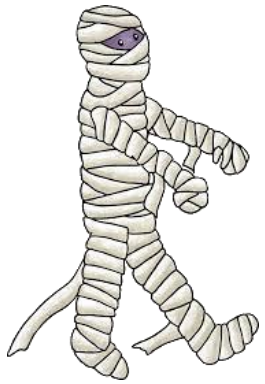
INTRODUCTION AUX PREUVES DE SÉCURITÉ

Cristina Onete
cristina.onete@gmail.com

INTERMEZZO : CRYPTER ET DECRYPTER

crypte



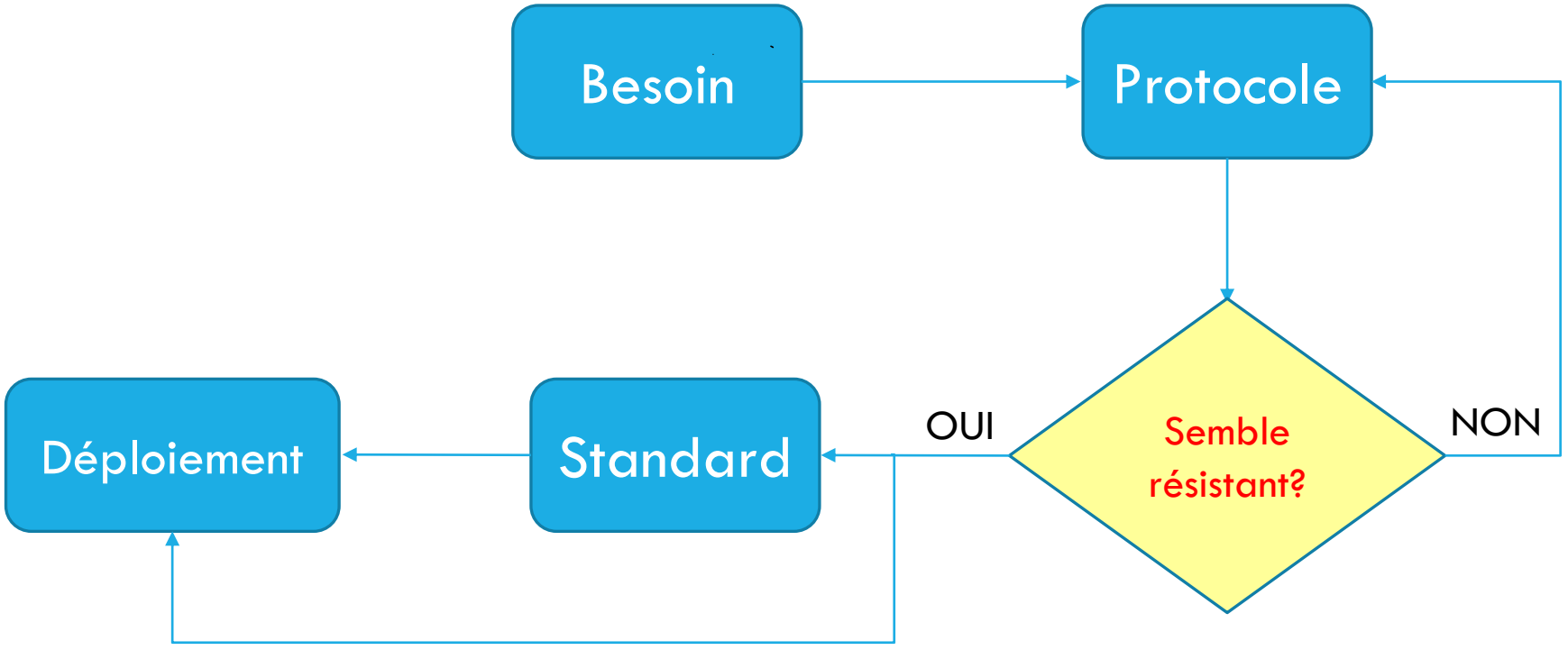


on crypte des

crypte-ographe

On CRYPTE les morts
On CHIFFRE les données

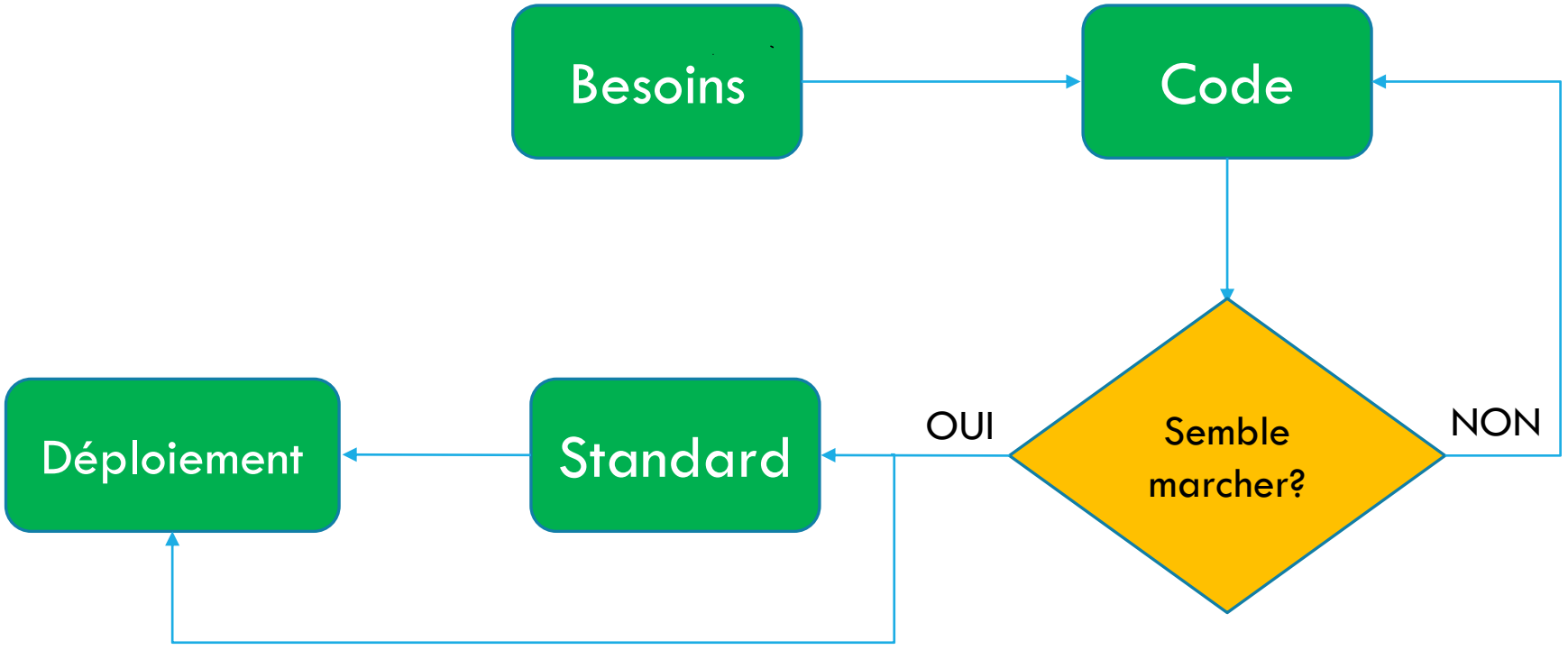
LA CRYPTO DES ANNÉES '90



JUSTE UN EXEMPLE : TLS

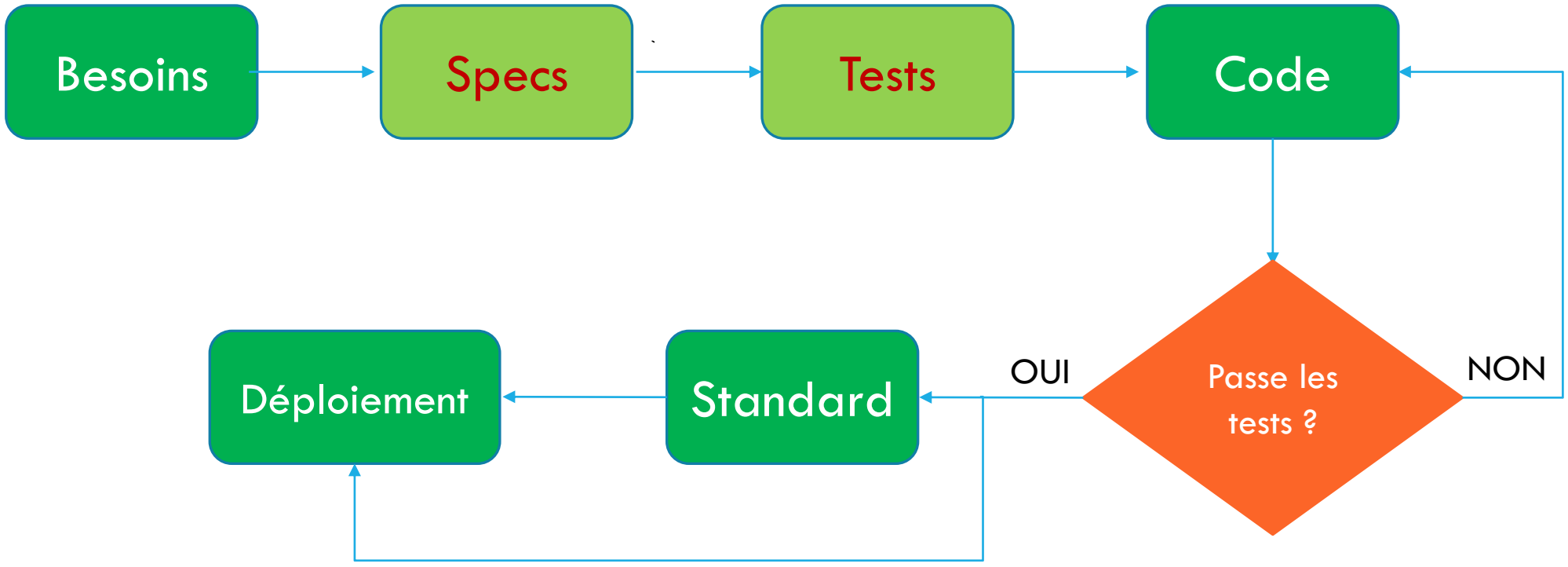
- Première version de TLS utilisée par Netscape : SSL 2.0
  - SSL 1.0 tellement susceptible aux failles qu'elle n'a jamais été mise en fonction
- SSL 2.0 remplacée très tôt par SSL 3.0
- TLS 1.2 : longtemps co-existante avec SSL 3.0, TLS 1.0…
- TLS 1.2 toujours vulnérable :
  - **Briques faibles** : MD5, cipher suites export (taille faible), RSA-PKCS, chiffrement CBC…
  - **Design faible** : même clé plusieurs propos, clé non-unique, trop de paramètres
  - **Implémentation faible** : problèmes de certification, anciennes versions possible, Heartbleed

COMME UN CODE SANS QUALITÉ



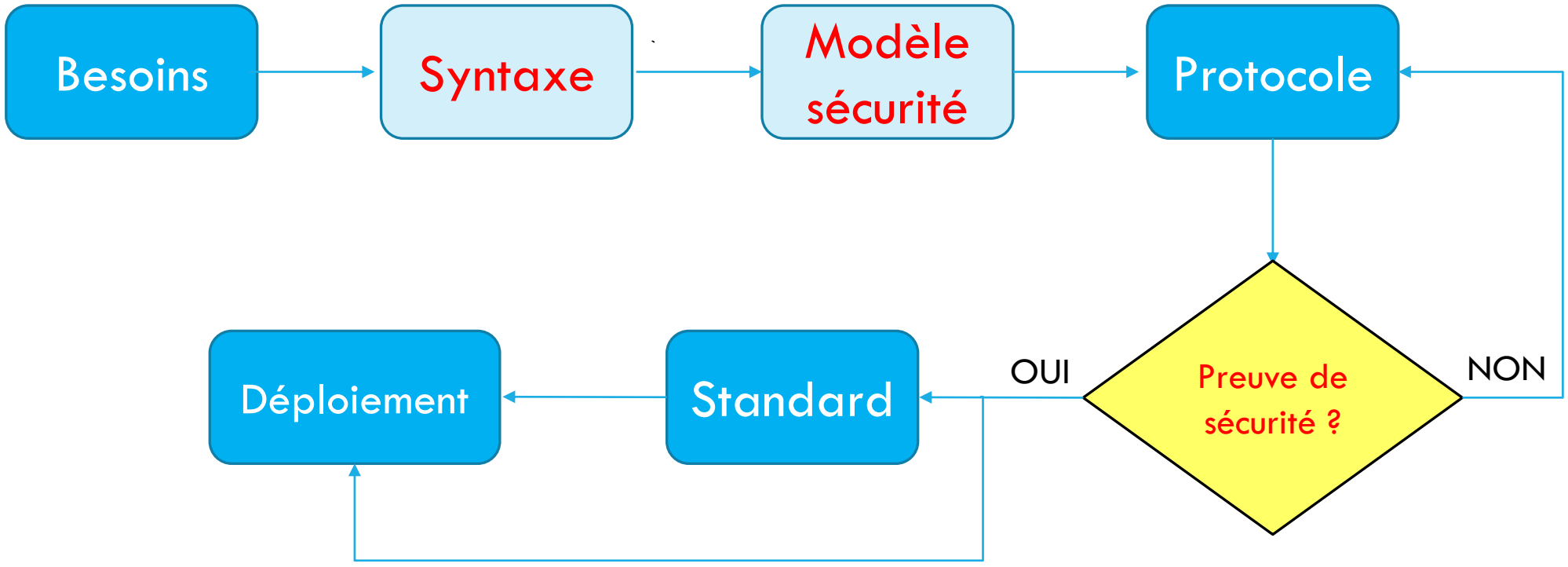
Code illisible, des failles, réponse partielle aux besoins…

TDD ET QUALITÉ DE CODE



➡ Un code de qualité qui répond aux besoins !

SECURITY BY DESIGN



Bienvenue à la sécurité prouvable !

LA SÉCURITÉ PROUVABLE

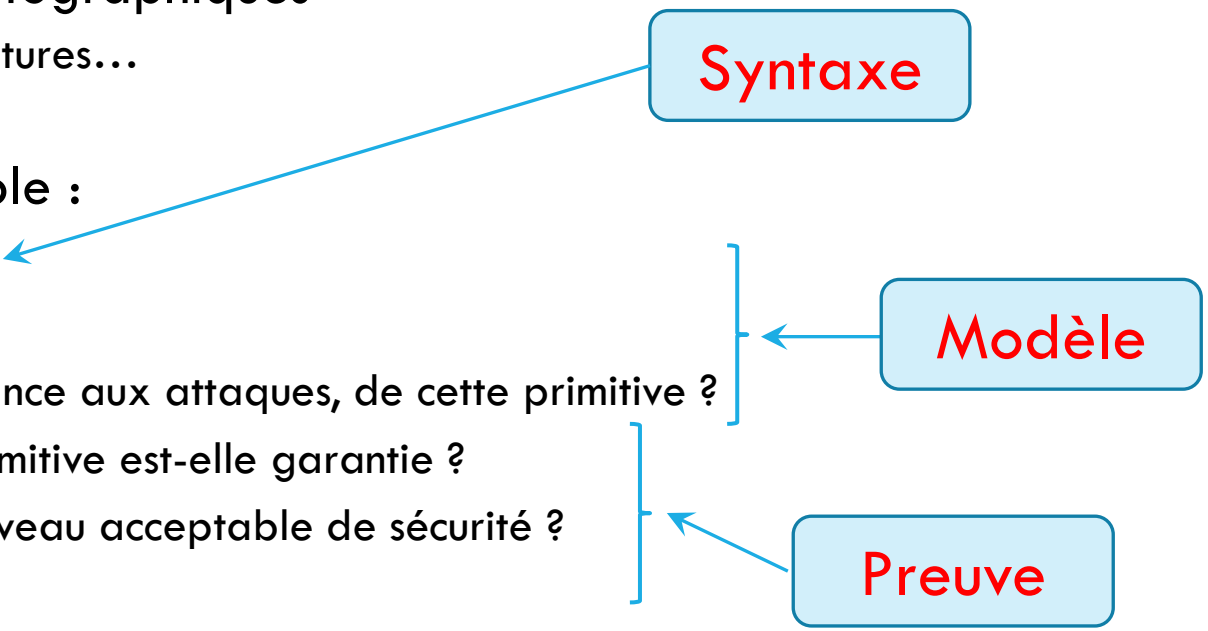
- Une méthodologie puissante
- Une garantie :
  - **Mathématique** : technique par réduction
  - **Précise** : la sécurité donnée est spécifiée par le modèle
  - **Universelle** : toute attaque dans le modèle
  - **Détaillée** : toute hypothèse connue et quantifiée
  - (Idéalement) **Exacte** : donne une indication sur la taille des paramètres
- Encourage un design propre, modulaire, se reposant sur des hypotheses connues
  - TLS 1.3 vs. TLS 1.2

SECURE BY DESIGN

CETTE OPTION

- Diverses primitives and protocoles cryptographiques
  - Fonctions de hachage, MAC, chiffrement, signatures…

- Le raisonnement de la sécurité prouvable :
  - Quel est le fonctionnement de cette primitive ?
  - Quel est son rôle en termes de sécurité ?
  - Quelles sont les limitations, en termes de résistance aux attaques, de cette primitive ?
  - Sous quelles hypothèses la sécurité de cette primitive est-elle garantie ?
  - Quelle instanciation de la primitive donne un niveau acceptable de sécurité ?



- Seuls pré-requis : intérêt pour la precision, raisonnement logique, proba. de base

STRUCTURE

- 12h CM, 18h TD :
  - Style mélangé : CM + exos, TDs + enseignement…
  - Matériel didactique : https://www.onete.net/teaching.html
  - Contact par mail : cristina.onete@gmail.com, parfois aussi via Discord
  - Dites moi si vous voulez que j'explique en anglais !!!
- Les CMs :
  - Aujourd'hui : introduction, à quoi ça sert, un exemple
  - Définitions de sécurité : chiffrement, signatures, hachage, authentification…
- TDs : bases de modélisation et de preuves

1 ***contrôle écrit*** 1ère session, 1 ***oral*** deuxième session

QUELQUES TERMES “MÉTIER”

LA SYNTAXE

- Décrit le fonctionnement d'une primitive/d'un protocole:
  - **Qu'est-ce qu**'une primitive de ce type ?
  - Ensemble d'**algorithmes ou procédures,** leurs entrées et sorties
  - **Fonctionnement** : propriétés de correctness/completeness

- **Exemple** : chiffrement à clé publique (PKE) -- triplet : PKE = (KGen, Enc, Dec) t.q. :
  - $(\mathrm{sk}, \mathrm{pk}) \leftarrow \mathrm{KGen}(1^{\lambda})$: génération de clés
  - $c \leftarrow \mathrm{Enc}(\mathrm{pk}; \mathrm{m})$: chiffrement à clé publique d'un texte clair m
  - $m \leftarrow \mathrm{Dec}(\mathrm{sk}; \mathrm{c})$: déchiffrement d'un texte chiffré c

- **Fonctionnement (correctness)** : $\forall m, \forall (\mathrm{sk}, \mathrm{pk}) \leftarrow \mathrm{KGen}(1^{\lambda}) : \mathrm{Dec}(\mathrm{Enc}(\mathrm{pk}; \mathrm{m}), \mathrm{sk}) = \mathrm{m}$

LE PRINCIPE DE KERCKHOFFS

La sécurité d'une primitive cryptographique ne doit jamais reposer sur le secret de ses algorithmes, sinon sur des clés secrètes. Il faut toujours supposer que tous les algorithmes seront publiques

Auguste Kerckhoffs

ADVERSAIRE, CHALLENGER, JEU

- **L'adversaire $\mathcal{A}$:** une/des entité.s ayant accès à une primitive cryptographique
  - Le but : **"casser" la sécurité** de la primitive en question

- Formalisation : deux formes principales :
  - Jeux de sécurité que $\mathcal{A}$ tente à gagner
  - Simulation : distinction entre un monde réel + adversaire et un monde idéal + simulateur

- Les jeux de sécurité :
  - Un adversaire joue le jeu contre un challenger (représentant les parties honnêtes)
  - Accès direct aux algorithmes, mais pas aux clés secrètes (Kerckhoffs)
  - Accès indirect aux clés et parties honnêtes : par oracle
  - Fin : le jeu s'arrête et l'adversaire gagne ou perd le jeu

LES JEUX DE SÉCURITÉ

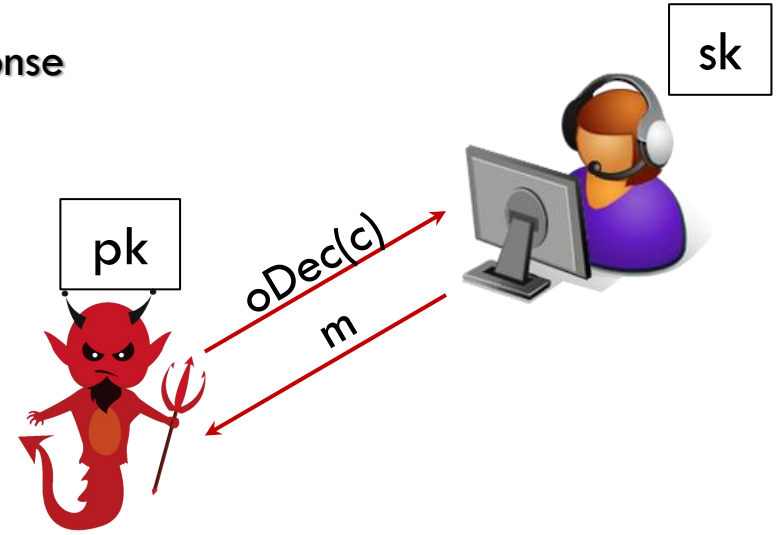
- Intuition :
  - Modéliser un adversaire “réaliste”
  - L’opposer à la primitive cryptographique, par des accès formalisés (algos, oracles)
  - Formaliser un but du jeu : casser la confidentialité, l’intégrité, usurper une identité, etc.

- **Exemple** : PKE = (KGen, Enc, Dec) :
  - $\mathscr{A}$ connaitra les algorithmes et les clés publiques de ses cibles
  - $\mathscr{A}$ peut connaitre des tuples (c, Dec(sk; c)) valides : accès par oracle
  - $\mathscr{A}$ gagne s’il réussit casser la confidentialité du schéma PKE
    - Plus difficile à définir qu’il ne semble

LE FONCTIONNEMENT DES ORACLES

- **Les oracles** :
  - Connaissance partielle du système
  - Exemple : oracle de déchiffrement
  - $\mathcal{A}$ fait une **requête** (query), l'oracle fait **un calcul** et retourne **une réponse**

- Exemple : PKE
  - L'algorithme KGen retourne (sk, pk), pk donnée à $\mathcal{A}$
  - Pas besoin d'un oracle pour Enc(pk; m)
  - Oracle oDec(c) avec c choisi par l'adversaire, calcule Dec(sk; c)



LE BUT DU JEU

- Le **pouvoir** de l'adeversaire peut varier :
  - Accès à plus ou moins d'oracles
  - Restrictions sur les requêtes possibles aux oracles
  - Buts du jeu différents

- Exemple : PKE
  - $\mathcal{A}$ ne connait pas m à partir d'un nouveau c (pas d'oracle)
  - $\mathcal{A}$ ne connait pas m à partir d'un nouveau c (oracle Dec)
  - IND-CPA : $\mathcal{A}$ ne connait aucun bit de m à partir de c
  - IND-CCA : $\mathcal{A}$ ne connait aucun bit de m à partir de c (oracles Dec)