Des mathématiques pour l'informatique

Itsaka Rakotonirina

INRIA Nancy Grand-Est

Prédiction 1

Au moins 4 personnes dans cette salle ont
leur anniversaire tombant le même mois

Prédiction 1

Au moins 4 personnes dans cette salle ont
leur anniversaire tombant le même mois

Pourquoi ?

Il y a **12** mois différents, donc si au plus **3** personnes
étaient du même mois, nous serions au plus **12** x **3** = 36

Prédiction 2

Au moins 6826 cartes bleues en France ont
le même code à 4 chiffres

Prédiction 2

Au moins 6826 cartes bleues en France ont
le même code à 4 chiffres

Pourquoi ?

Même chose : il y a **10000** codes différents,
et **68,250,000** cartes bleues en circulation

Dans la vraie vie

Théorie

Produire des connaissance

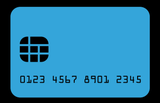
Prédiction

En déduire les conséquences logiques sur le monde

Sécurité

Réagir si besoin

Sécurité et informatique

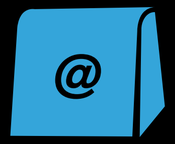


carte bleue

téléphone

avion

satellite



box internet

passeport
biométrique

clés de voiture

centrale

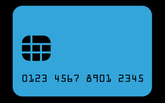
Erreurs / Accidents

satellite

avion

centrale

Piratage



carte bleue

téléphone

passeport biométrique

clés de voiture

box internet

Des maths pour la sécurité

Solide 

Arguments rigoureux et précis

Vérifiable ✓

On peut relire les arguments,
contrôler qu’ils sont valides

Des maths pour la sécurité

Solide 

Arguments rigoureux et précis

Vérifiable ✓

On peut relire les arguments,
contrôler qu'ils sont valides

→ **Fondements de la confiance**

Dans la vraie vie

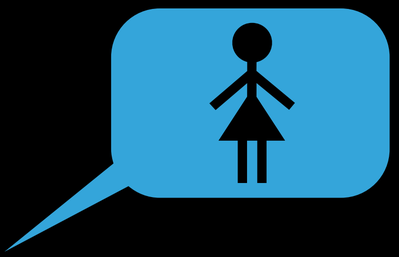
Extrait de la loi Suisse

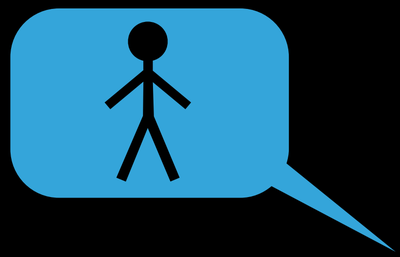
(*Exigences techniques et administratives applicables au vote électronique*,
en vigueur depuis le 15 janvier 2014)

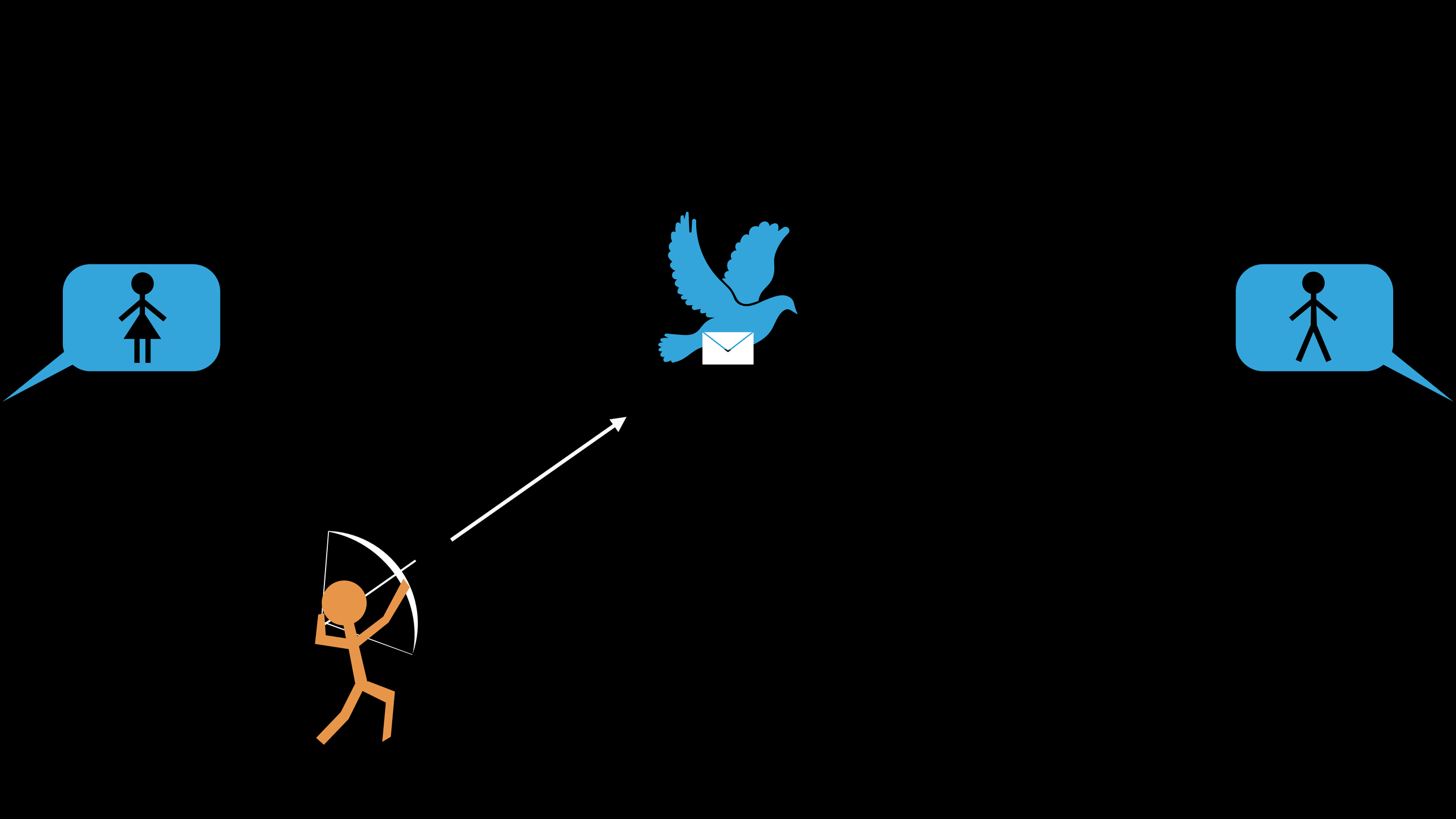
5.1. Contrôle du protocole cryptographique

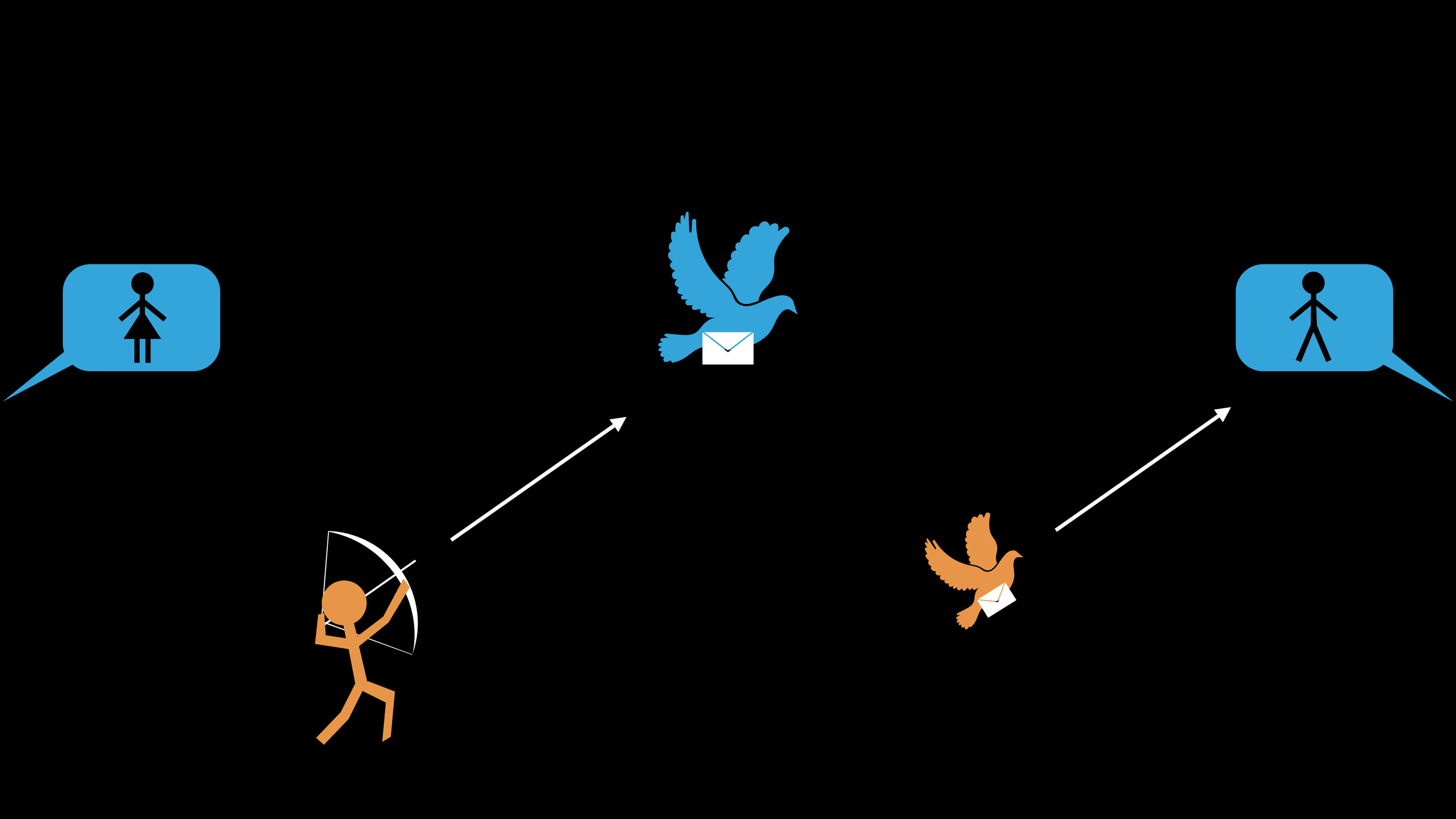
5.1.1	Critères de contrôle: le protocole doit être conforme à l'objectif de sécurité et aux hypothèses de confiance figurant dans le modèle abstrait décrit au ch. 4. Pour cela, il doit exister une preuve cryptographique et une preuve symbolique. En ce qui concerne les composants cryptographiques fondamentaux, les preuves peuvent être apportées sur la base des hypothèses de sécurité généralement admises (par exemple « random oracle model », « decisional Diffie-Hellman assumption » et « Fiat-Shamir heuristic »). Le protocole doit se fonder si possible sur des protocoles éprouvés.

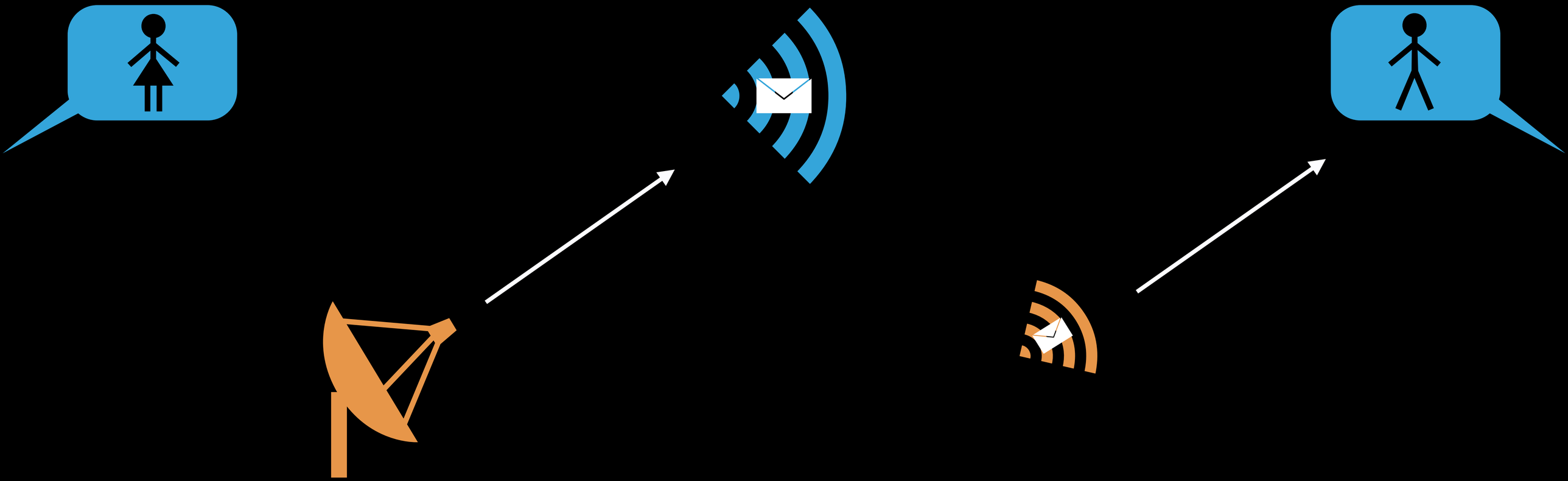
Les protocoles cryptographiques



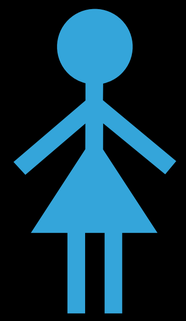


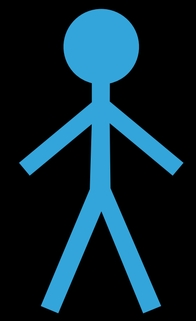






Protéger les communications

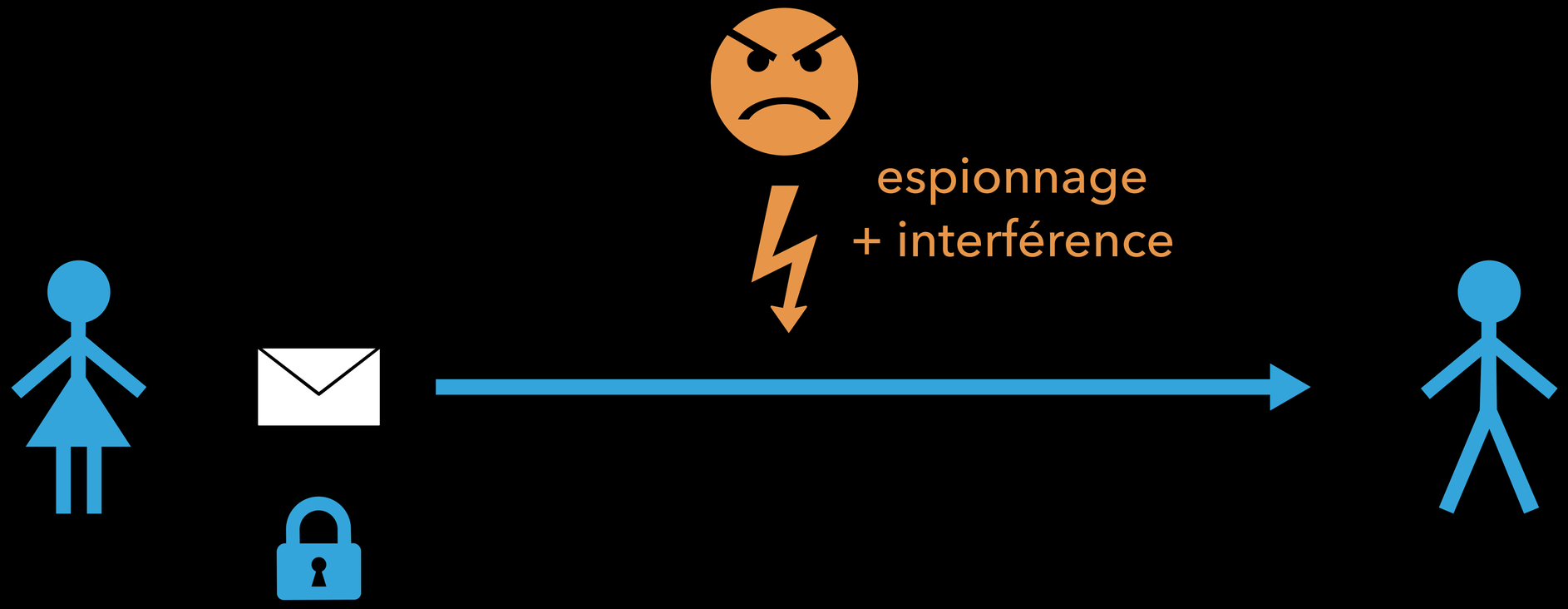




Protéger les communications

Protéger les communications

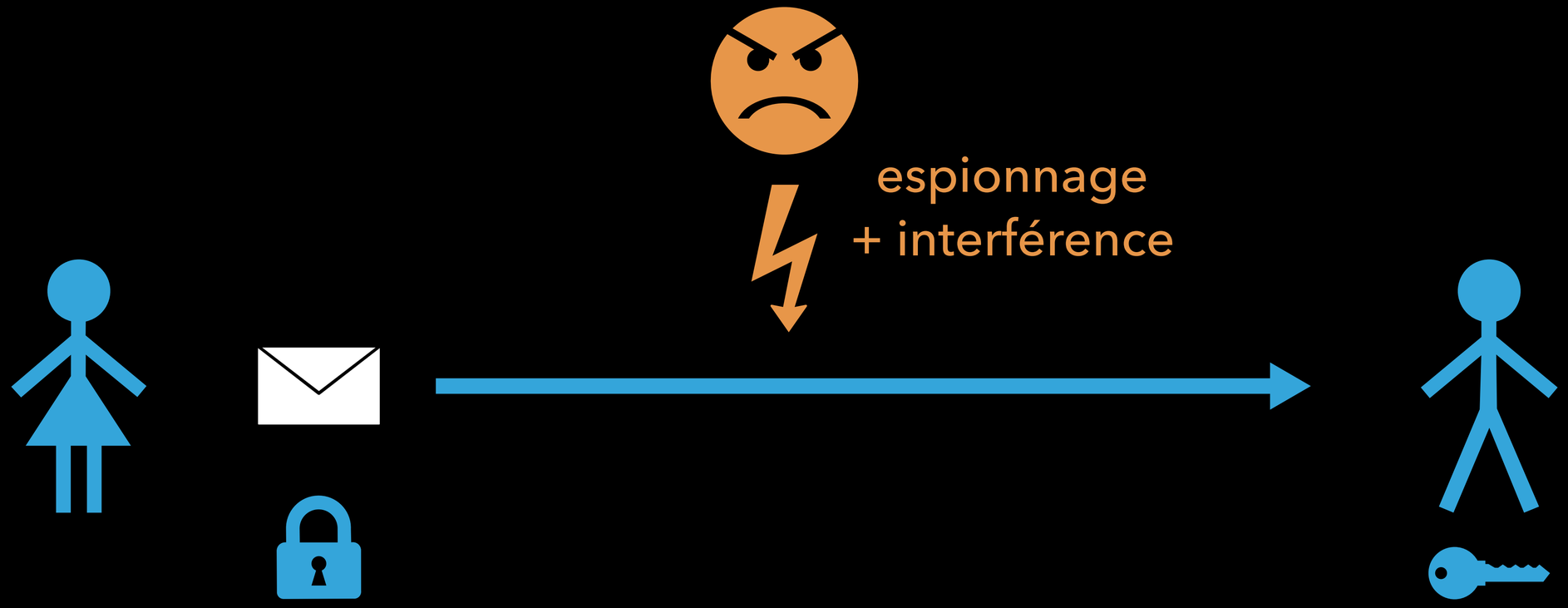
Protéger les communications



chiffrement

= rendre le message incompréhensible

Protéger les communications



chiffrement

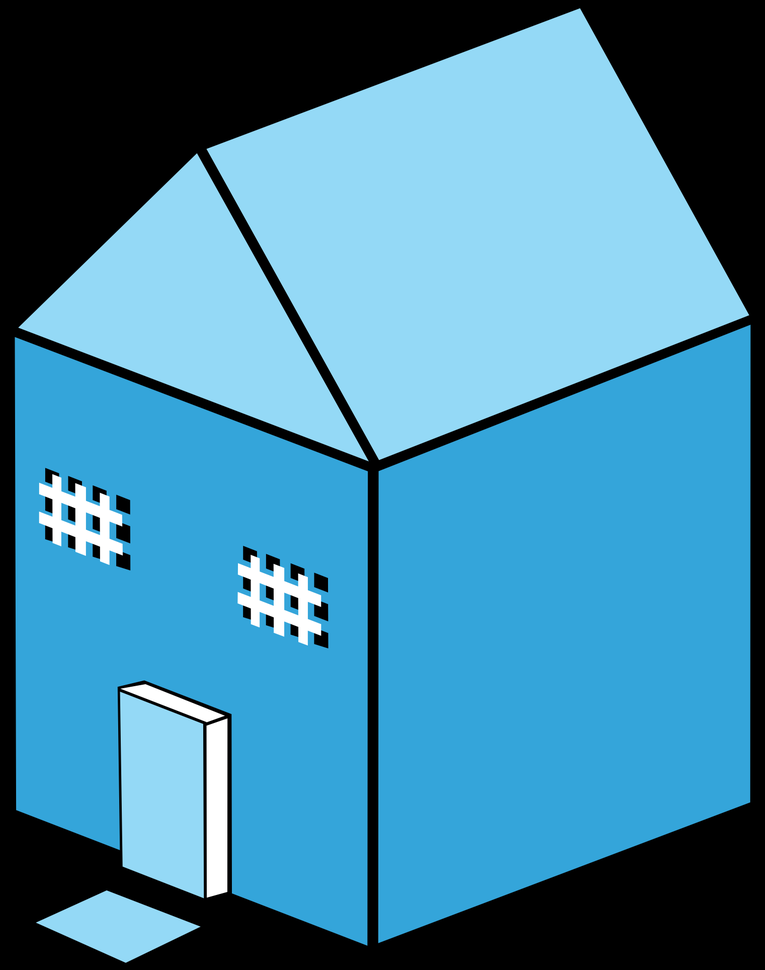
= rendre le message incompréhensible

déchiffrement

= récupérer le message

MAIS

- ✓ Porte blindée
- ✓ Fenêtres à barreaux



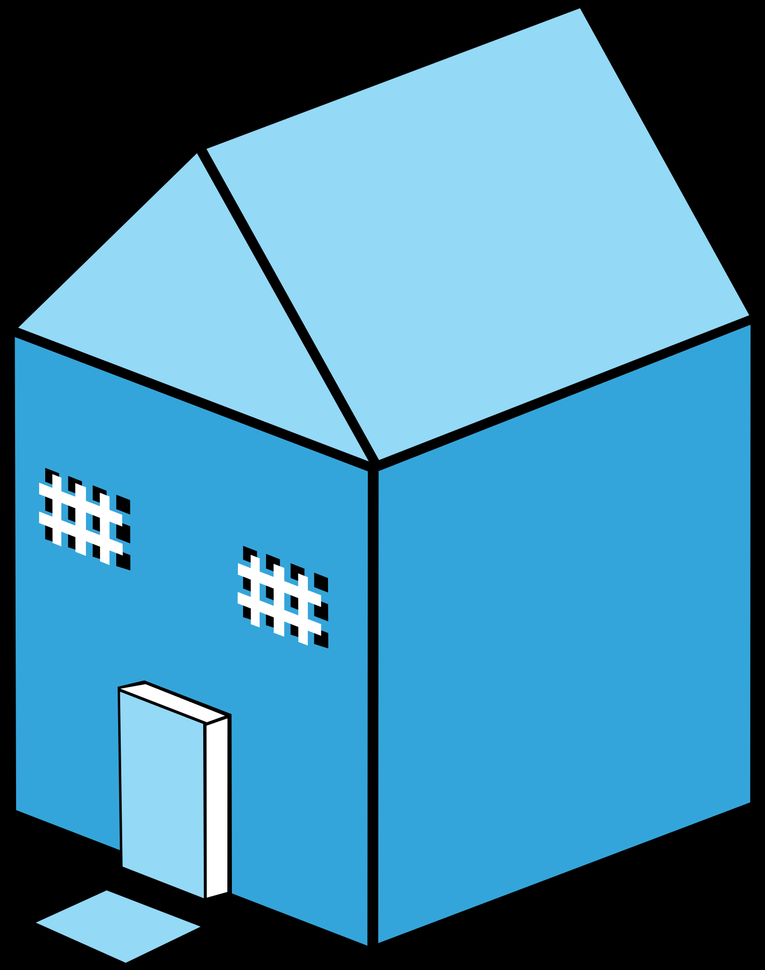
✓ Porte blindée

✓ Fenêtres à barreaux

mais…

☠ Clé sous le paillasson

☠ On dit “c’est moi” à l’interphone



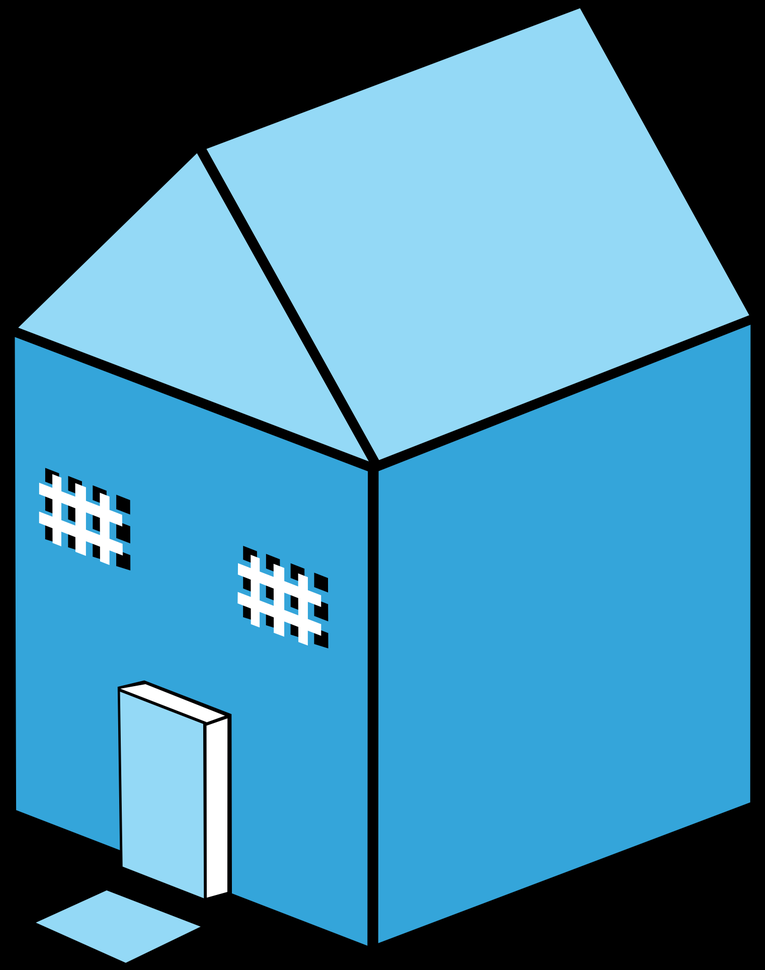
✓ Porte blindée

✓ Fenêtres à barreaux

mais…

☠ Clé sous le paillasson

☠ On dit “c’est moi” à l’interphone

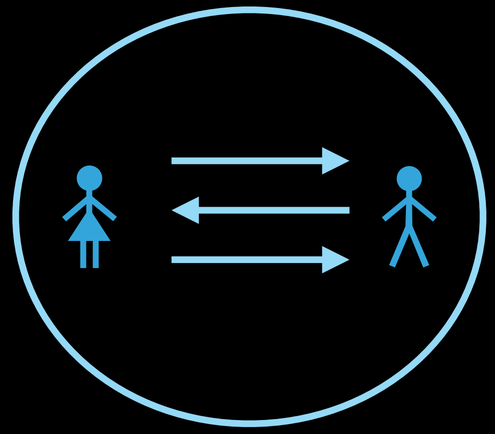


→ Peu importe la qualité du matériel de protection s’il est mal utilisé

Bilan : la sécurité a de nombreux visages

Cryptographie

mécanismes de protection



Protocoles

mécanismes de communication

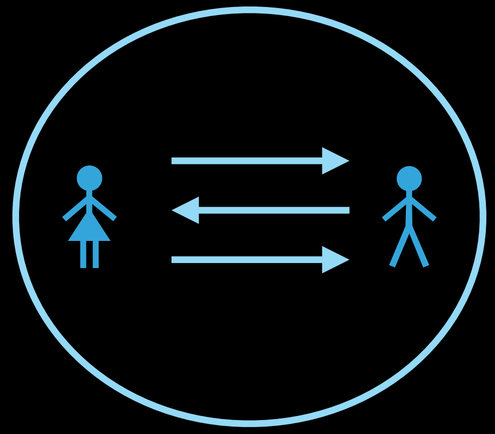
et beaucoup
d'autres...

Bilan : la sécurité a de nombreux visages

Cryptographie

mécanismes de protection

arithmétique



Protocoles

mécanismes de communication

logique

et beaucoup
d'autres...

En résumé

La conclusion

- Programmes informatiques partout
- Lourdes conséquences en cas de faille de sécurité
- ⇒ nécessité de garanties rigoureuses

La conclusion

- Programmes informatiques partout
- Lourdes conséquences en cas de faille de sécurité
- ⇒ nécessité de garanties ***rigoureuses***

*= Être **précis** sur ce qu'on veut prouver et sur les arguments qu'on utilise*