Cyber-sécurité
&
intelligence artificielle

Brice Colombier, Damien Robissout

Univ Lyon, UJM-Saint-Etienne, CNRS, Laboratoire Hubert Curien UMR 5516

Pint of Science, 20 mai 2019

Présentation

Damien Robissout, doctorant

- université de BORDEAUX — Master Cryptologie et Sécurité Informatique

Brice Colombier, post-doctorant

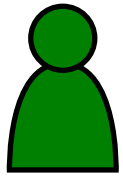
- télécom saint-étienne école d'ingénieurs / nouvelles technologies — École d'ingénieur, spécialité électronique
- INSA LYON — Master, spécialité électronique/systèmes embarqués
- Université de Lyon | Université Jean Monnet Saint-Étienne — Doctorat en micro-électronique

Définition : protection des données échangées sur un réseau.

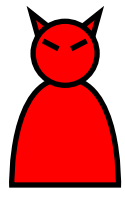
Objectifs : disponibilité, intégrité, authenticité, **confidentialité**.

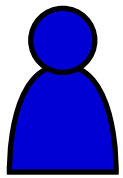
Confidentialité : A et B communiquent sans que C ne comprenne.

Chiffrement symétrique

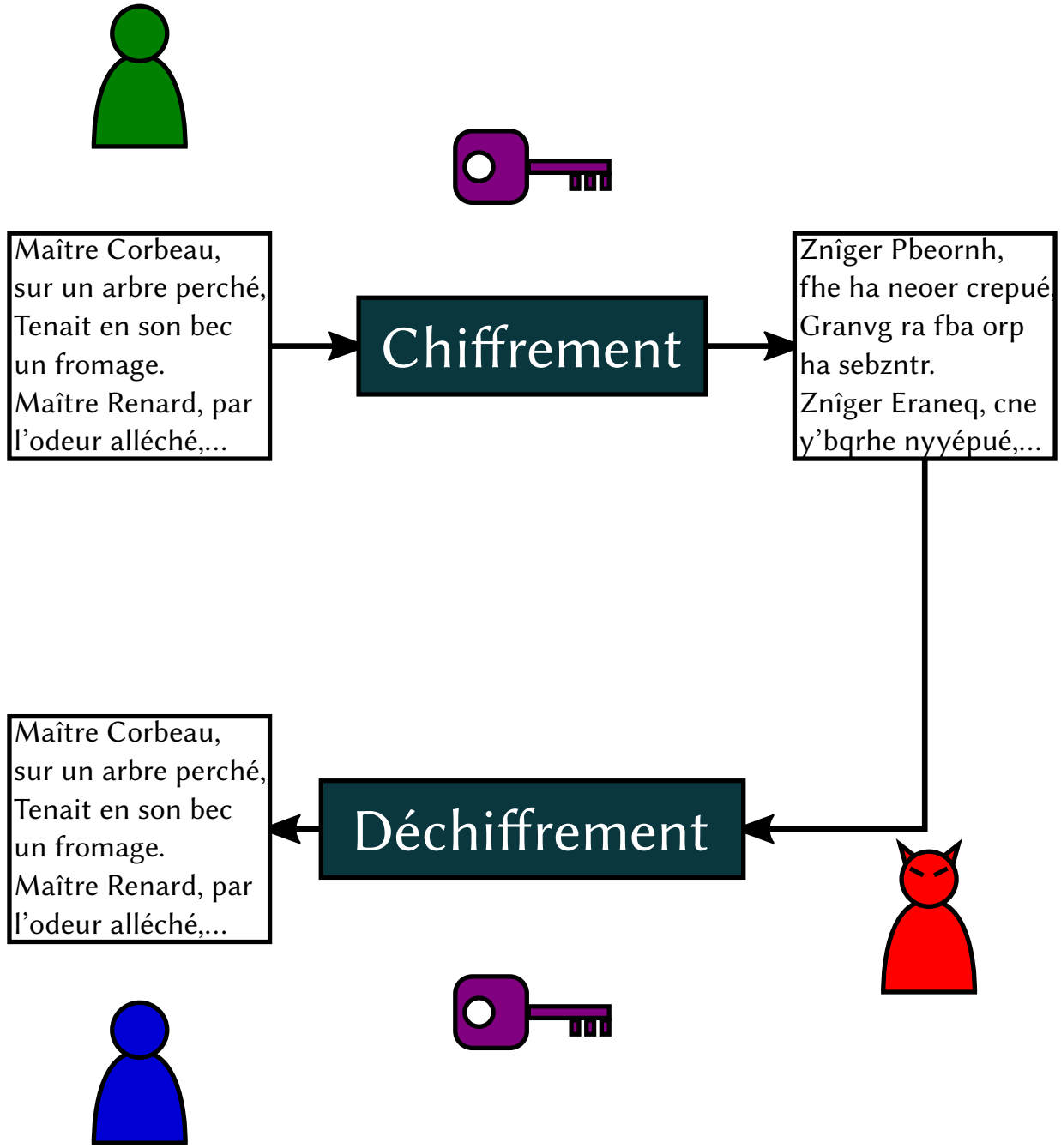


Maître Corbeau,
sur un arbre perché,
Tenait en son bec
un fromage.
Maître Renard, par
l'odeur alléché,...

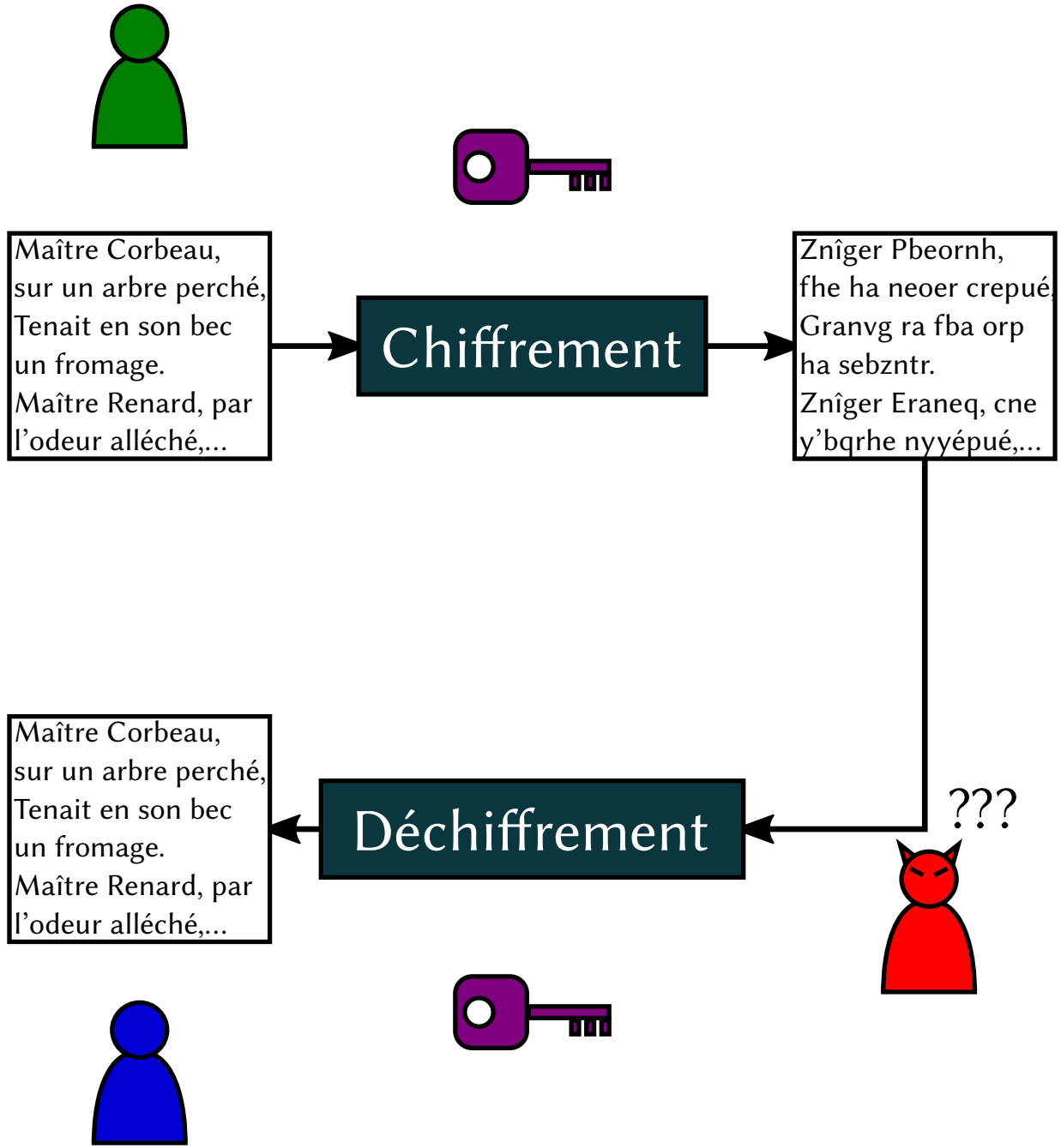




Chiffrement symétrique



Chiffrement symétrique



Chiffrement symétrique

- Clé **secrète** devant être préalablement **partagée**.
- Exemples de méthodes de chiffrement symétrique :
  - Chiffrement de César

    Clé : chiffre entre 1 et 25

    ➜ 25 possibilités

Chiffrement symétrique

- Clé **secrète** devant être préalablement **partagée**.
- Exemples de méthodes de chiffrement symétrique :
  - Chiffrement de César

    Clé : chiffre entre 1 et 25

    ➔ 25 possibilités
  - Advanced Encryption Standard

    Clé : suite de 128 bits (0/1)

    ➔ 2^{128} possibilités

$$\overbrace{(2 \times 2 \times 2 \times \ldots \times 2)}^{128}$$

Chiffrement symétrique

- Clé **secrète** devant être préalablement **partagée**.
- Exemples de méthodes de chiffrement symétrique :
  - Chiffrement de César

    Clé : chiffre entre 1 et 25

    ➔ 25 possibilités
  - Advanced Encryption Standard

    Clé : suite de 128 bits (0/1)

    ➔ 2^{128} possibilités $\left(\overbrace{2 \times 2 \times 2 \times \ldots \times 2}^{128}\right)$

    ➔ 340 milliards de milliards de millards de millards de possibilités

Chiffrement symétrique

- Clé **secrète** devant être préalablement **partagée**.
- Exemples de méthodes de chiffrement symétrique :
  - Chiffrement de César

    Clé : chiffre entre 1 et 25

    ➜ 25 possibilités
  - Advanced Encryption Standard

    Clé : suite de 128 bits (0/1)

    ➜ 2^{128} possibilités $\left(\overbrace{2 \times 2 \times 2 \times \ldots \times 2}^{128}\right)$

    ➜ 340 milliards de milliards de millards de millards de possibilités

    ➜ 10 milliards d'ordinateurs, testant 80 milliards de clés par seconde, depuis la naissance de l'Univers

Chiffrement symétrique

- Clé **secrète** devant être préalablement **partagée**.
- Exemples de méthodes de chiffrement symétrique :
  - Chiffrement de César

    Clé : chiffre entre 1 et 25

    ➜ 25 possibilités
  - Advanced Encryption Standard

    Clé : suite de 128 bits (0/1)

    ➜ 2^{128} possibilités $\overbrace{(2 \times 2 \times 2 \times \ldots \times 2)}^{128}$

    ➜ 340 milliards de milliards de millards de millards de possibilités

    ➜ 10 milliards d'ordinateurs, testant 80 milliards de clés par seconde, depuis la naissance de l'Univers

    ➜ Une goutte dans 10 mille milliards d'océans.

Chiffrement symétrique

- Clé **secrète** devant être préalablement **partagée**.
- Exemples de méthodes de chiffrement symétrique :
  - Chiffrement de César

    Clé : chiffre entre 1 et 25

    ➜ 25 possibilités
  - Advanced Encryption Standard

    Clé : suite de 128 bits (0/1)

    ➜ 2^{128} possibilités $\left(\overbrace{2 \times 2 \times 2 \times \ldots \times 2}^{128}\right)$

    ➜ 340 milliards de milliards de millards de millards de possibilités

    ➜ 10 milliards d'ordinateurs, testant 80 milliards de clés par seconde, depuis la naissance de l'Univers

    ➜ Une goutte dans 10 mille milliards d'océans.

    ➜ … bref, c'est beaucoup

Sécurité mathématique

Impossible de tester toutes les clés pour retrouver la bonne

Sécurité matérielle

Le chiffrement est **mis en œuvre** dans un système électronique :

- ordinateur,
- smartphone,
- carte bancaire…

Contrainte physique

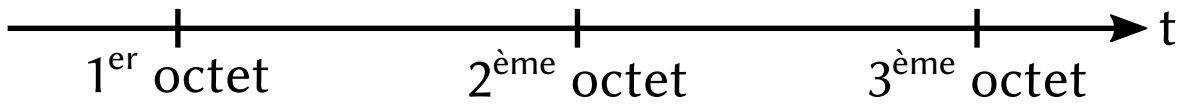
La clé de **128 bits** est manipulée par blocs de **8 bits (octets)**.

Le chiffrement est **mis en œuvre** dans un système électronique :

- ordinateur,
- smartphone,
- carte bancaire…

Contrainte physique

La clé de **128 bits** est manipulée par blocs de **8 bits (octets)**.

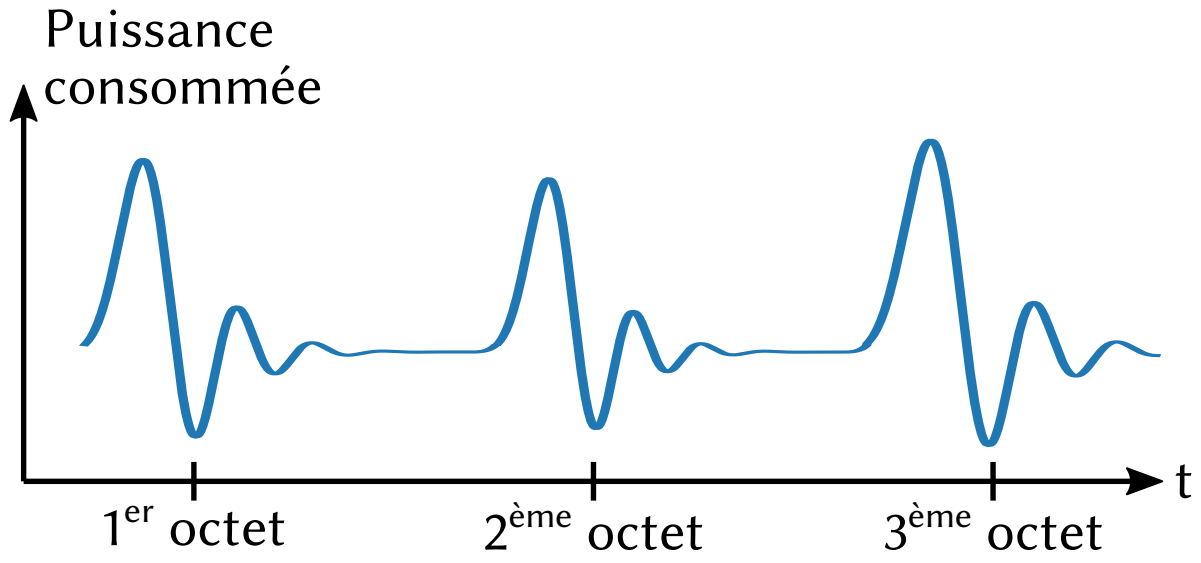


Le chiffrement est **mis en œuvre** dans un système électronique :

- ordinateur,
- smartphone,
- carte bancaire…

Contrainte physique

La clé de **128 bits** est manipulée par blocs de **8 bits (octets)**.

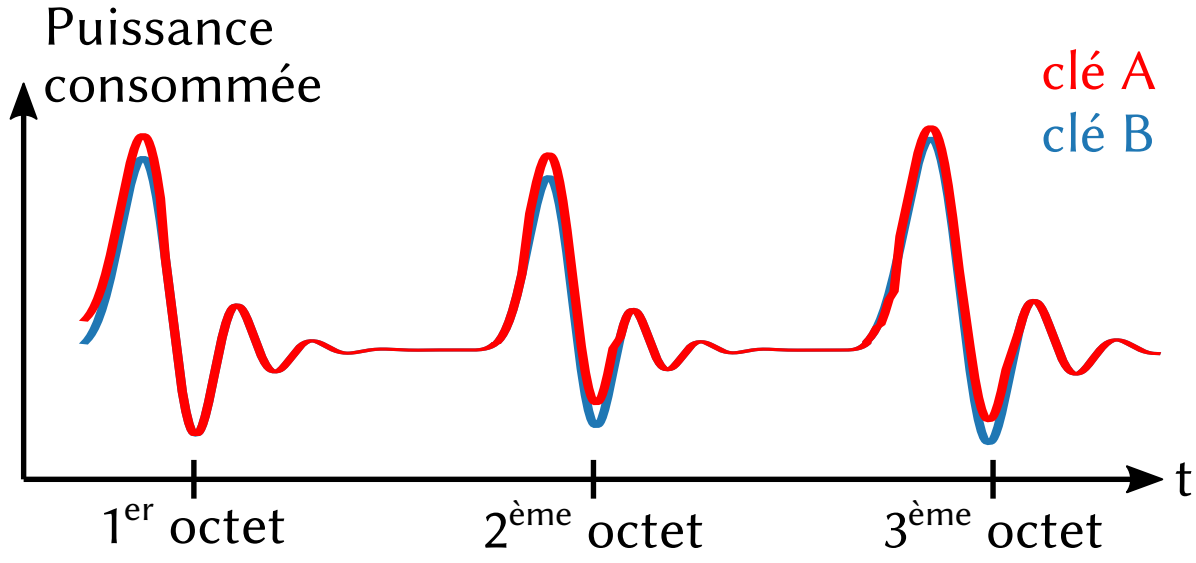


Le chiffrement est **mis en œuvre** dans un système électronique :

- ordinateur,
- smartphone,
- carte bancaire…

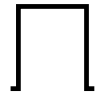
Contrainte physique

La clé de **128 bits** est manipulée par blocs de **8 bits (octets)**.



Principes

- La puissance consommée **dépend** de la donnée manipulée
- La donnée manipulée est manipulée **par morceaux**

Valeur de l'octet	Puissance consommée
0	
1	
2	
…	
255	

Puissance consommée	Valeur de l'octet
	?

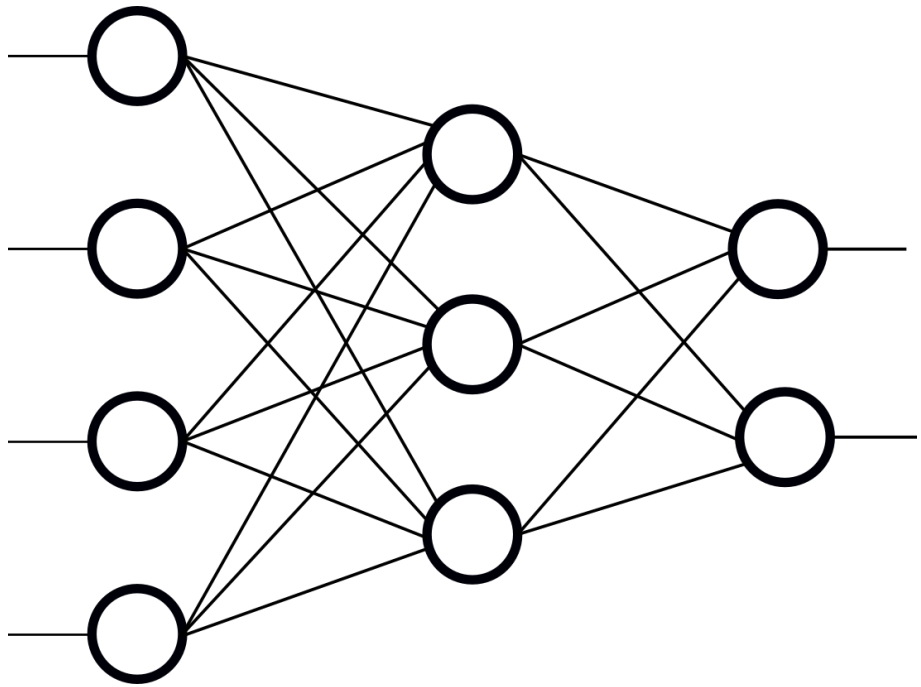
Réseaux de neurones

Définition : Ensemble de neurones interconnectés.

Objectif : Résoudre un problème de classification.

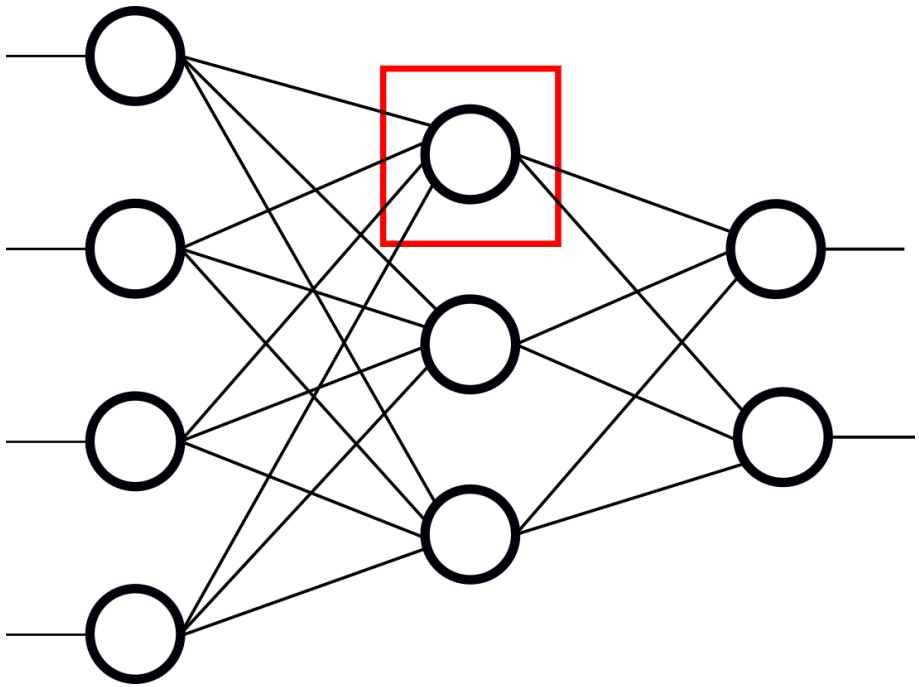
Méthode : Apprendre à partir d'exemples connus.

Exemple : Multi Layer Percetron (MLP) ou perceptron multicouche en français.



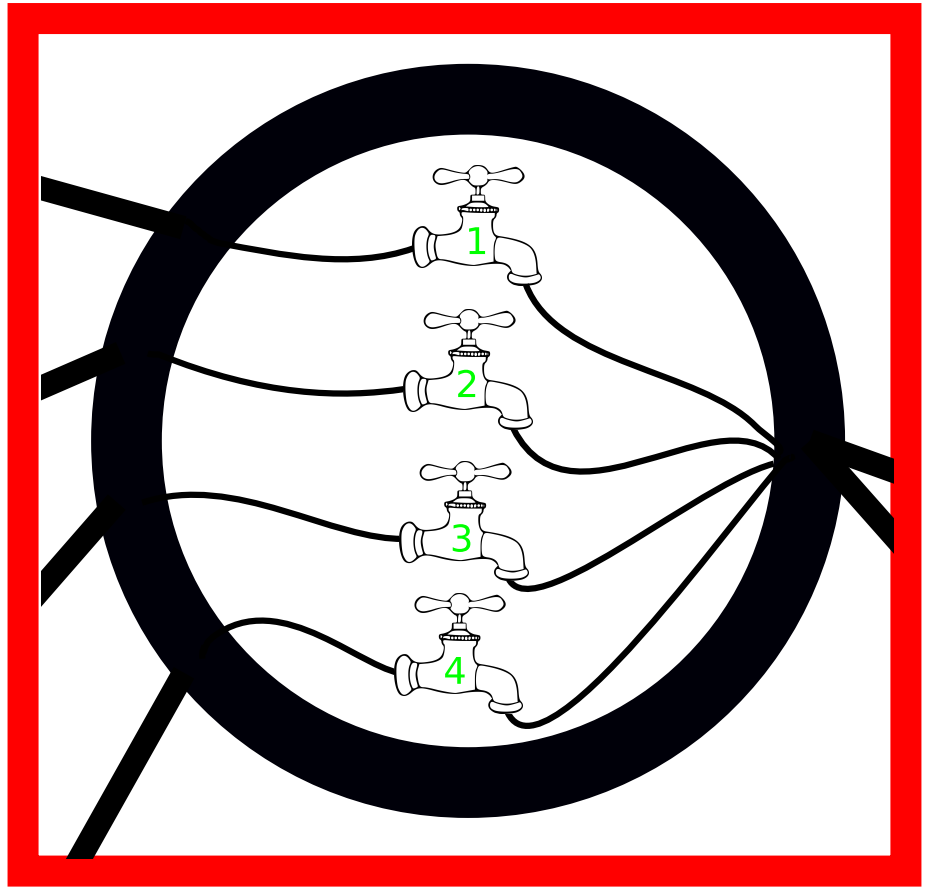
Mais qu’est ce qu’un neurone ?

Exemple : Multi Layer Percetron (MLP) ou perceptron multicouche en français.



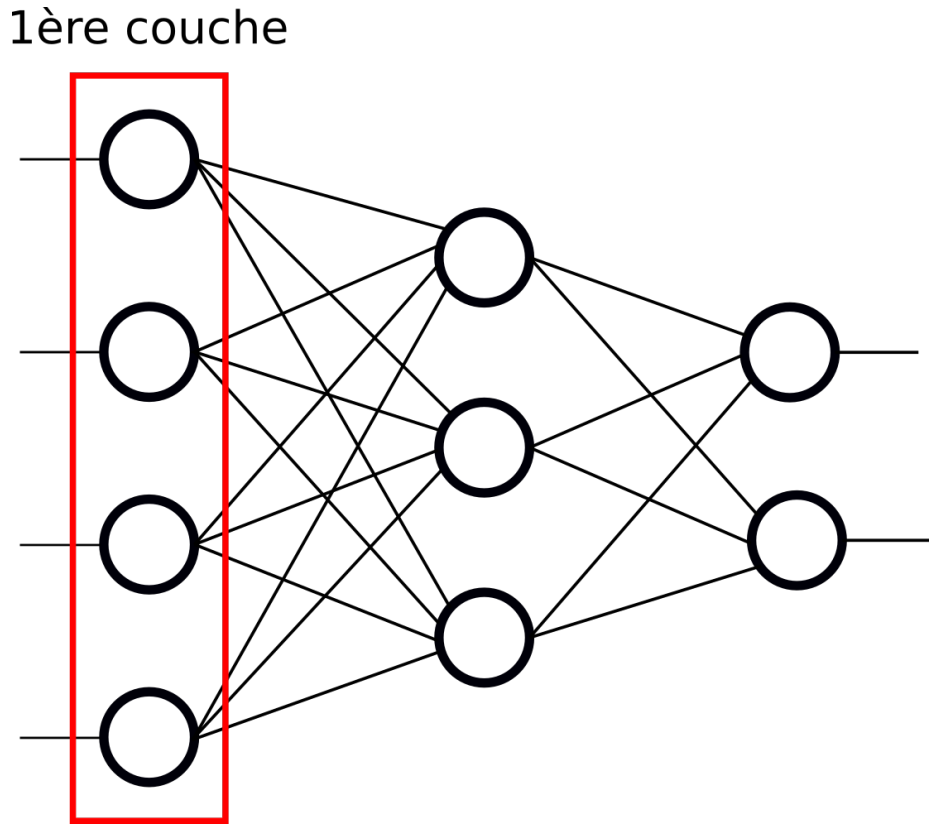
Mais qu'est ce qu'un neurone ?

Zoom sur l’intérieur d’un neurone



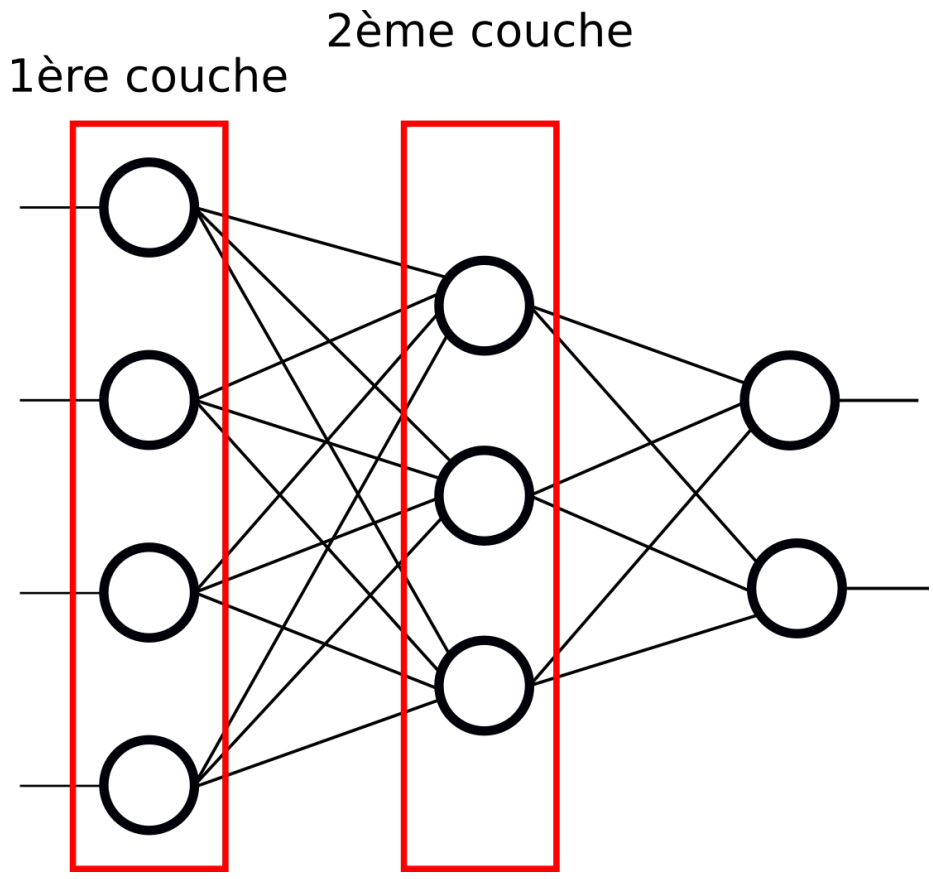
Réseaux de neurones

Un réseaux de neurones, comment ça marche ?



Avec un système de couches !

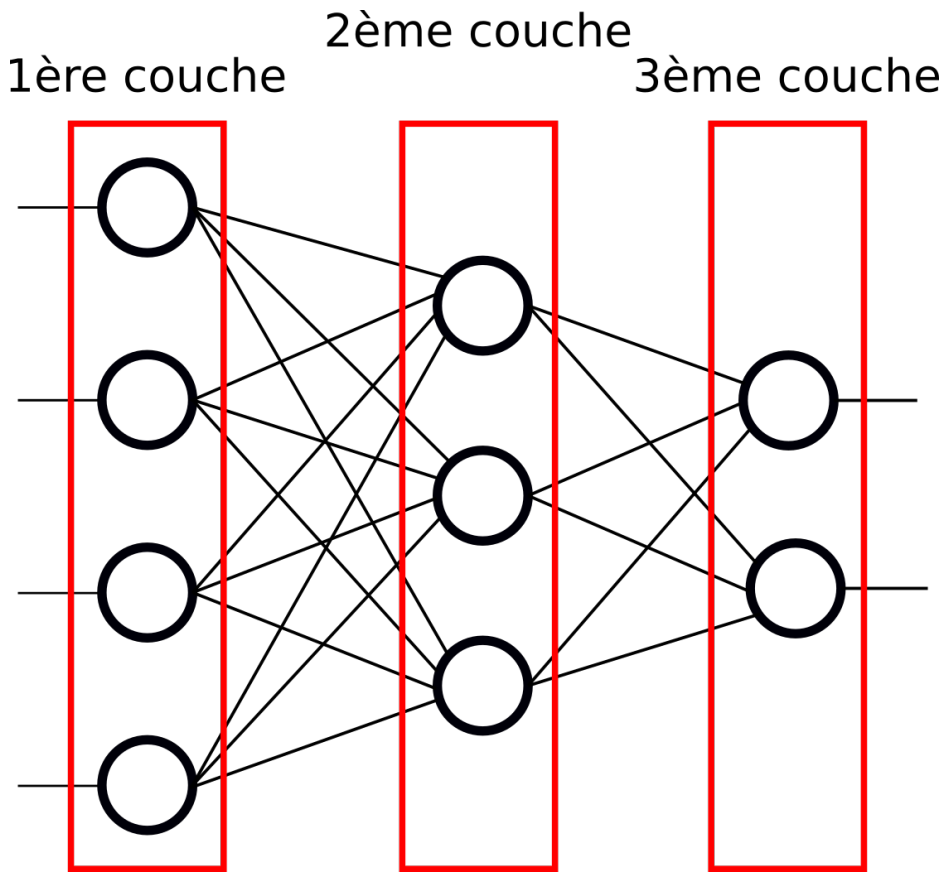
Un réseaux de neurones, comment ça marche ?



Avec un système de couches !

Réseaux de neurones

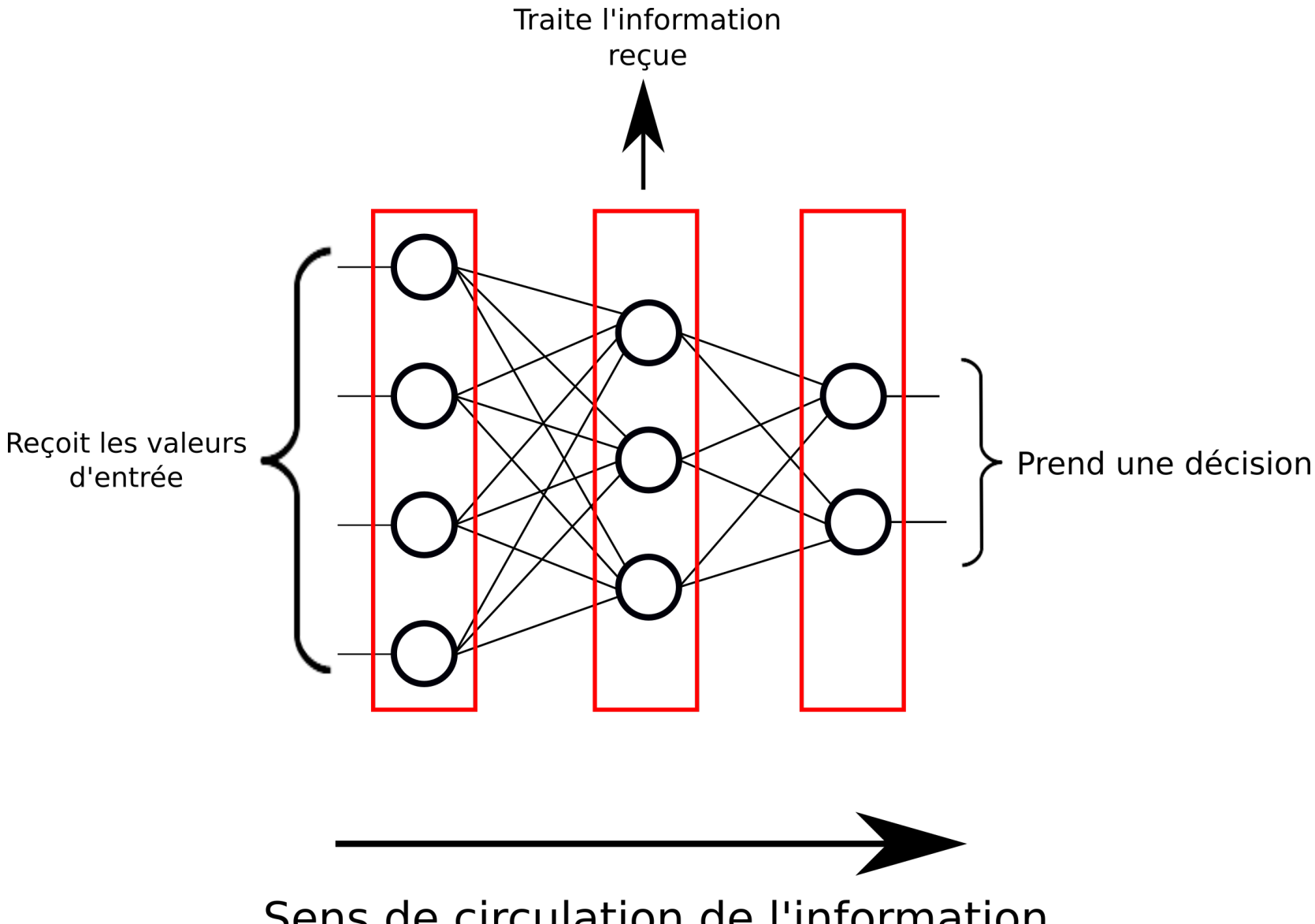
Un réseaux de neurones, comment ça marche ?



Avec un système de couches !

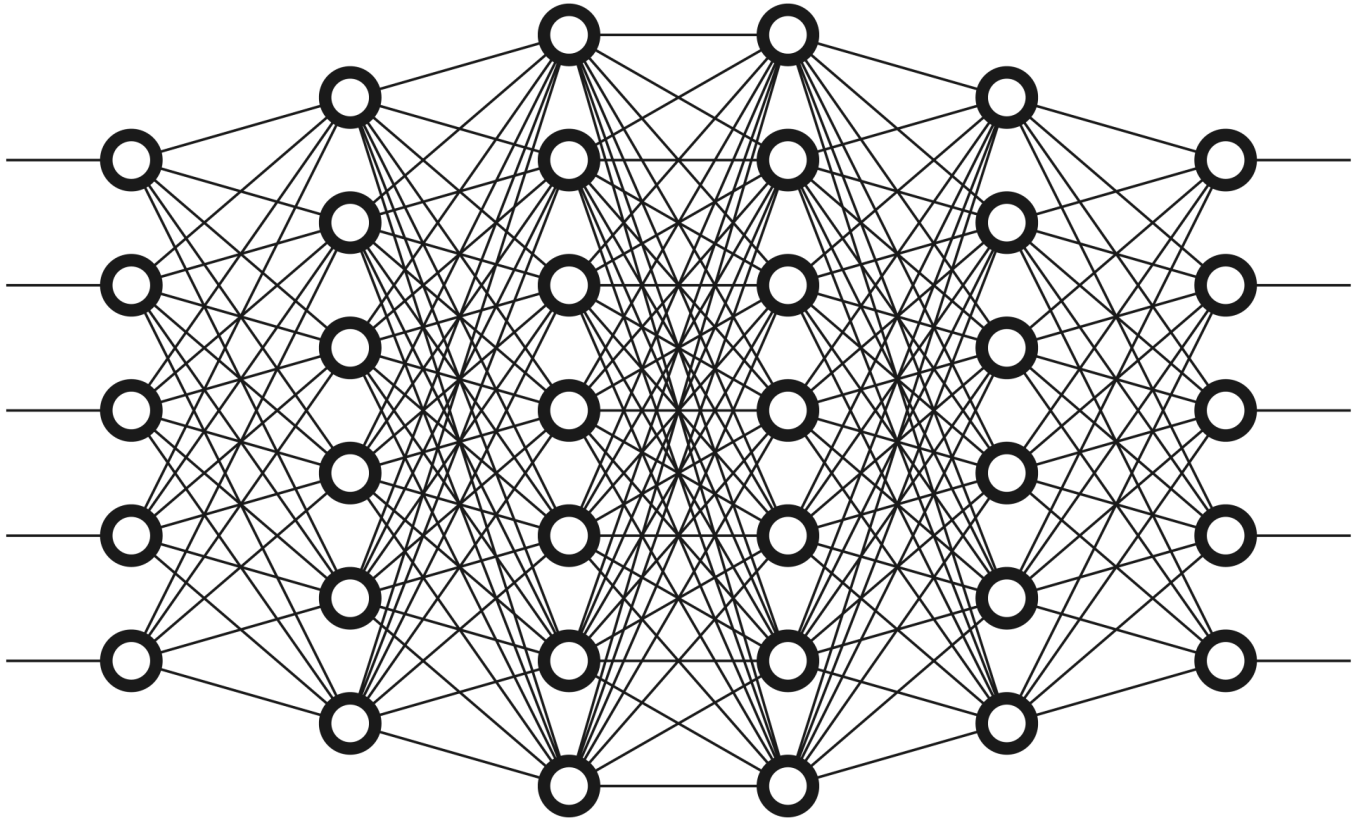
Réseaux de neurones

Un réseaux de neurones, comment ça marche ?



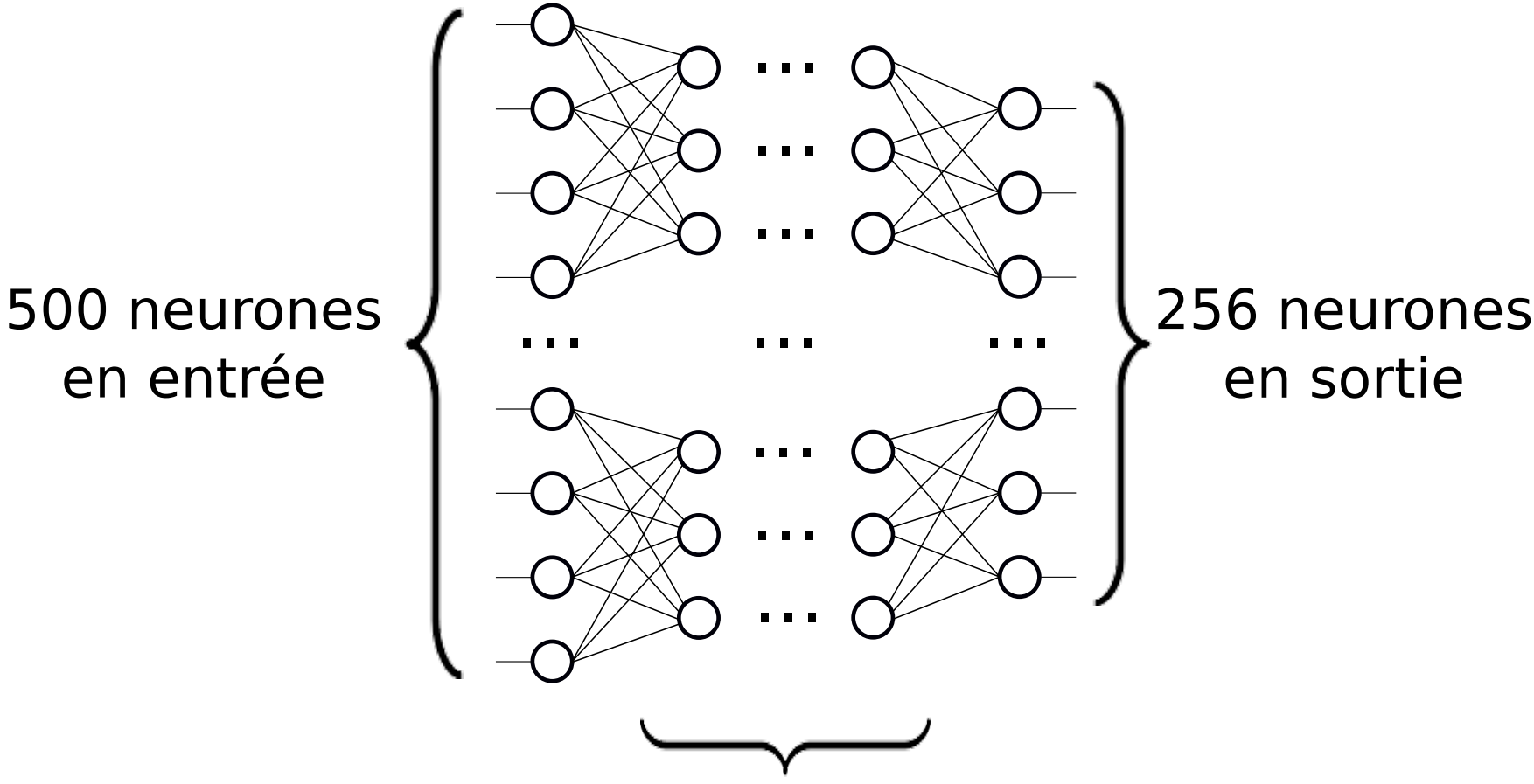
Réseaux de neurones complexes

On augmente un peu la complexité ?

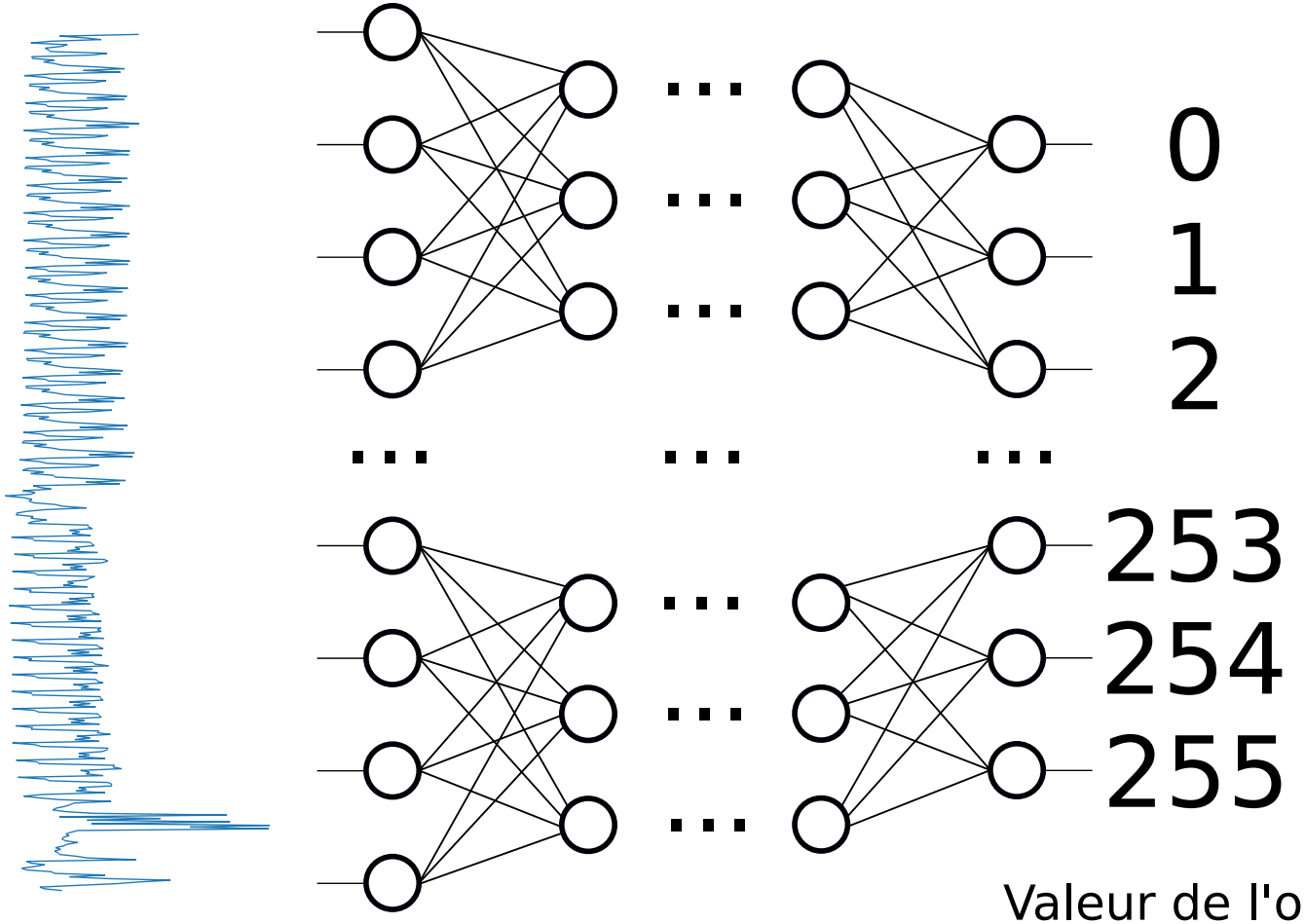


Plus il y a de couches et de neurones, plus il y a de connexions !

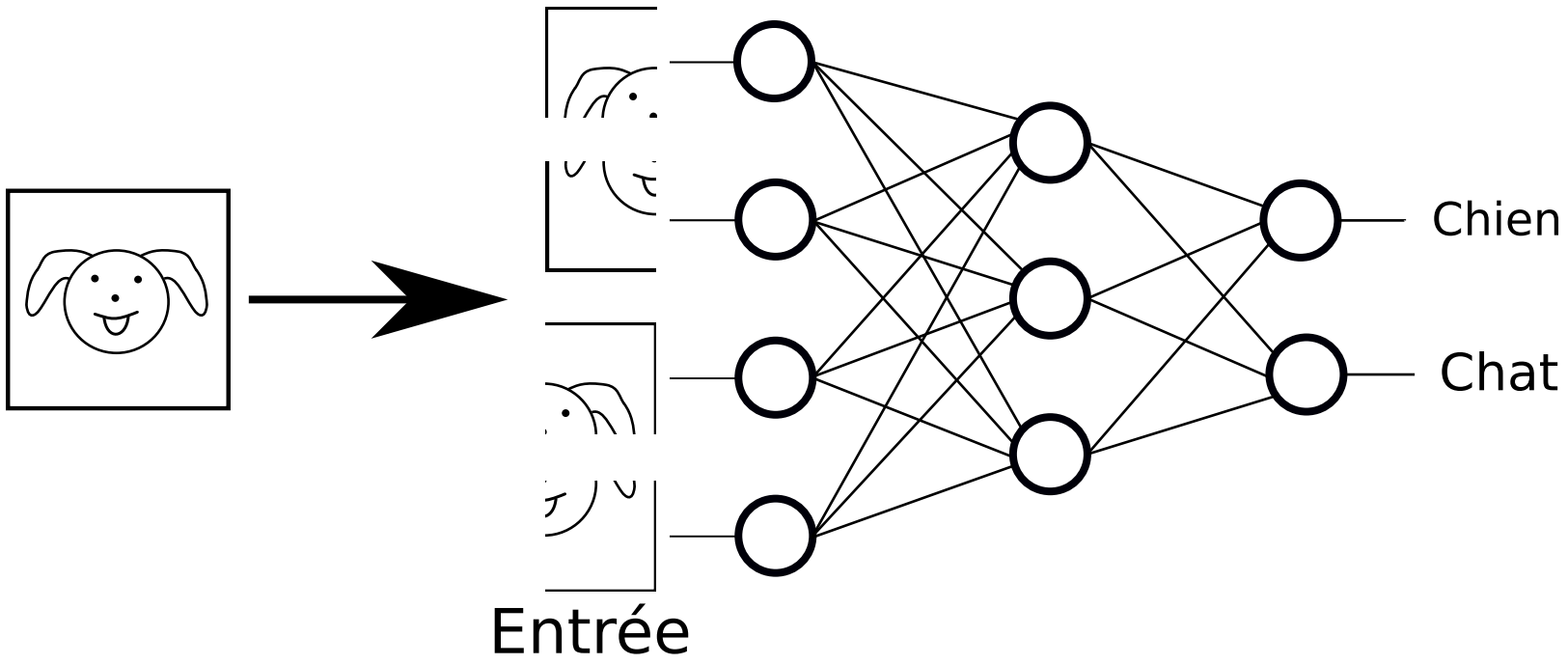
Application à notre problème



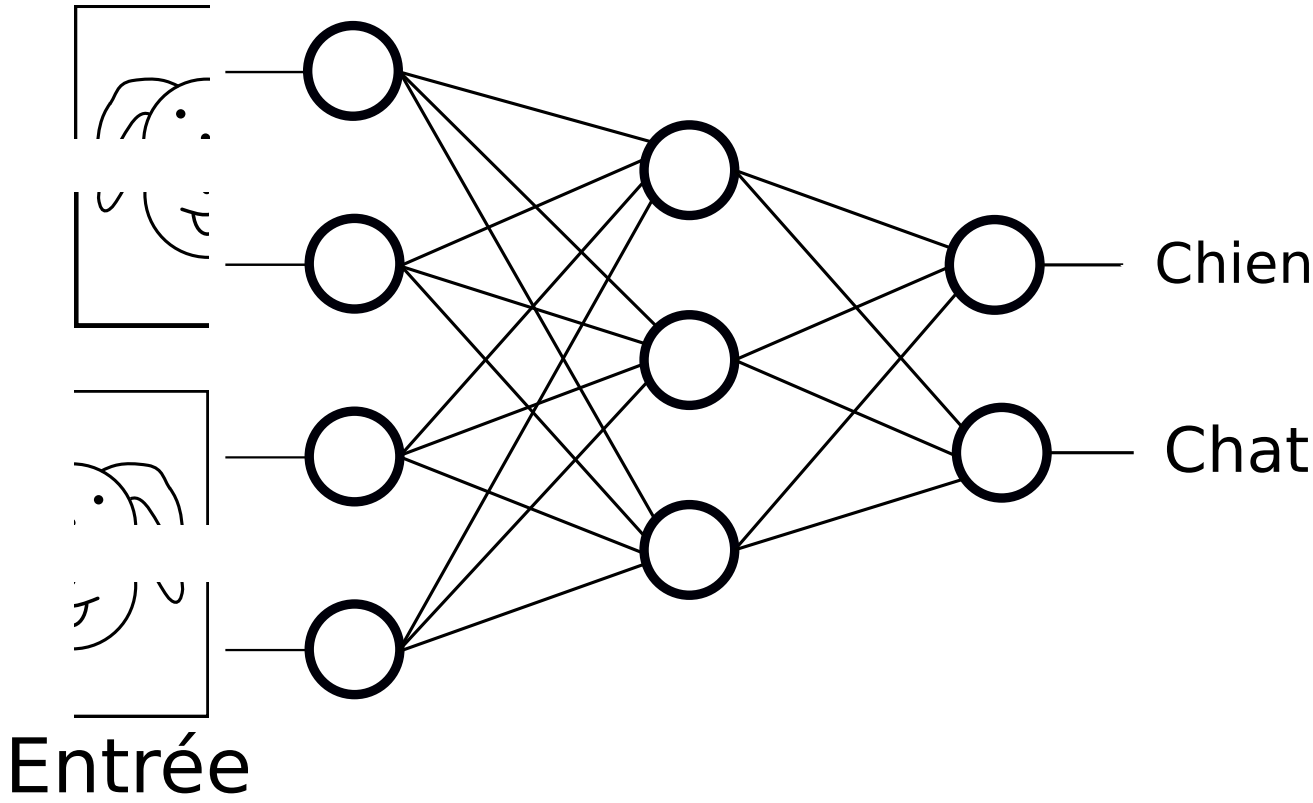
Application à notre problème



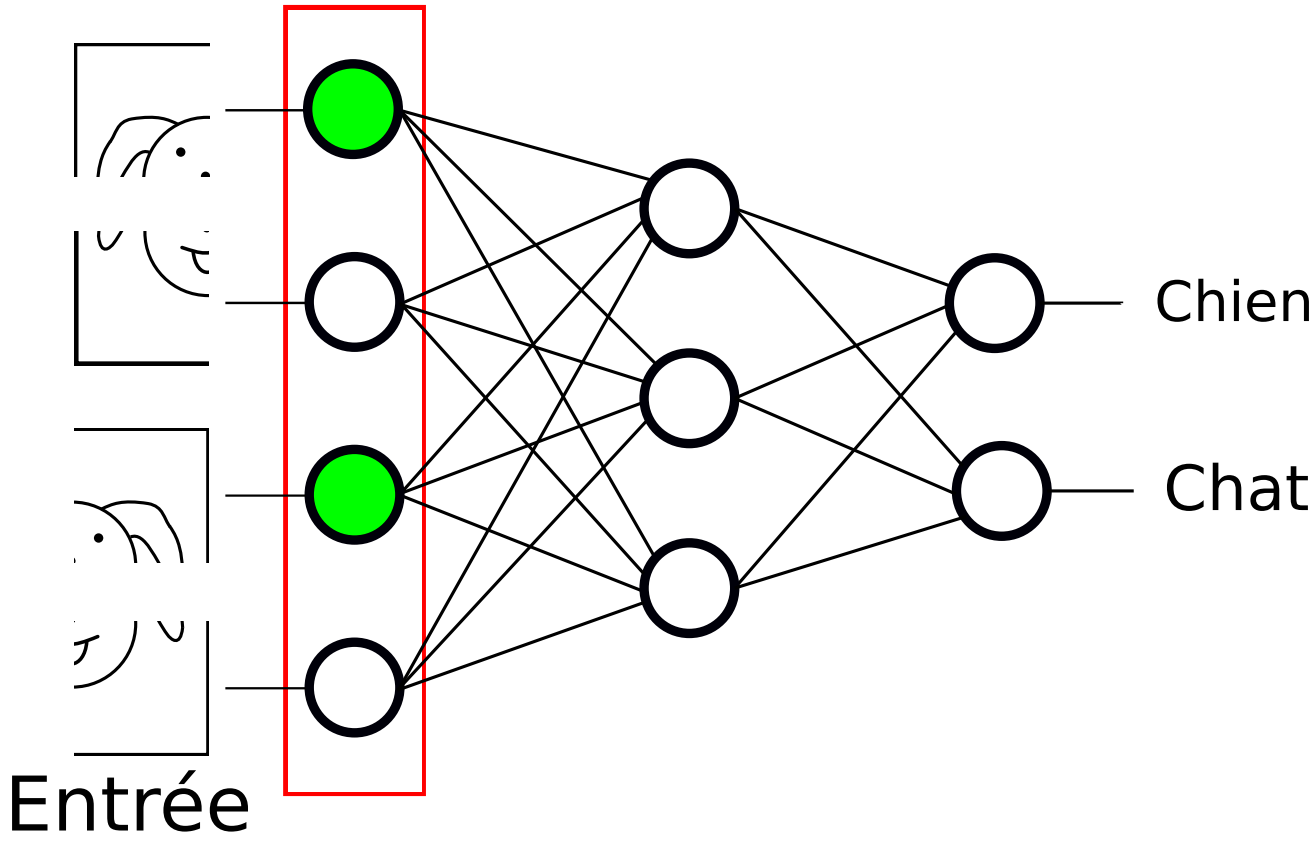
Exemple de réseaux de neurones (1)



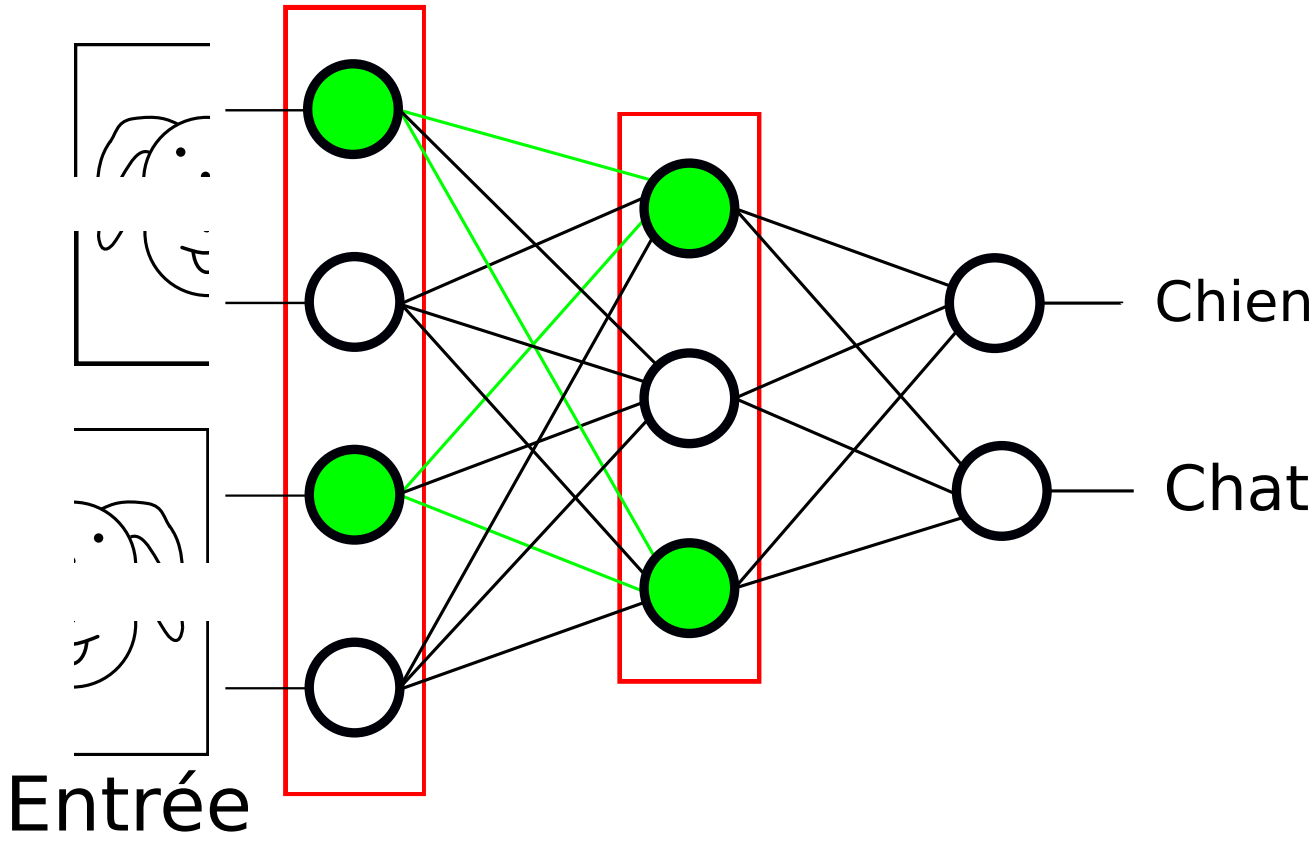
Exemple de réseaux de neurones (1)



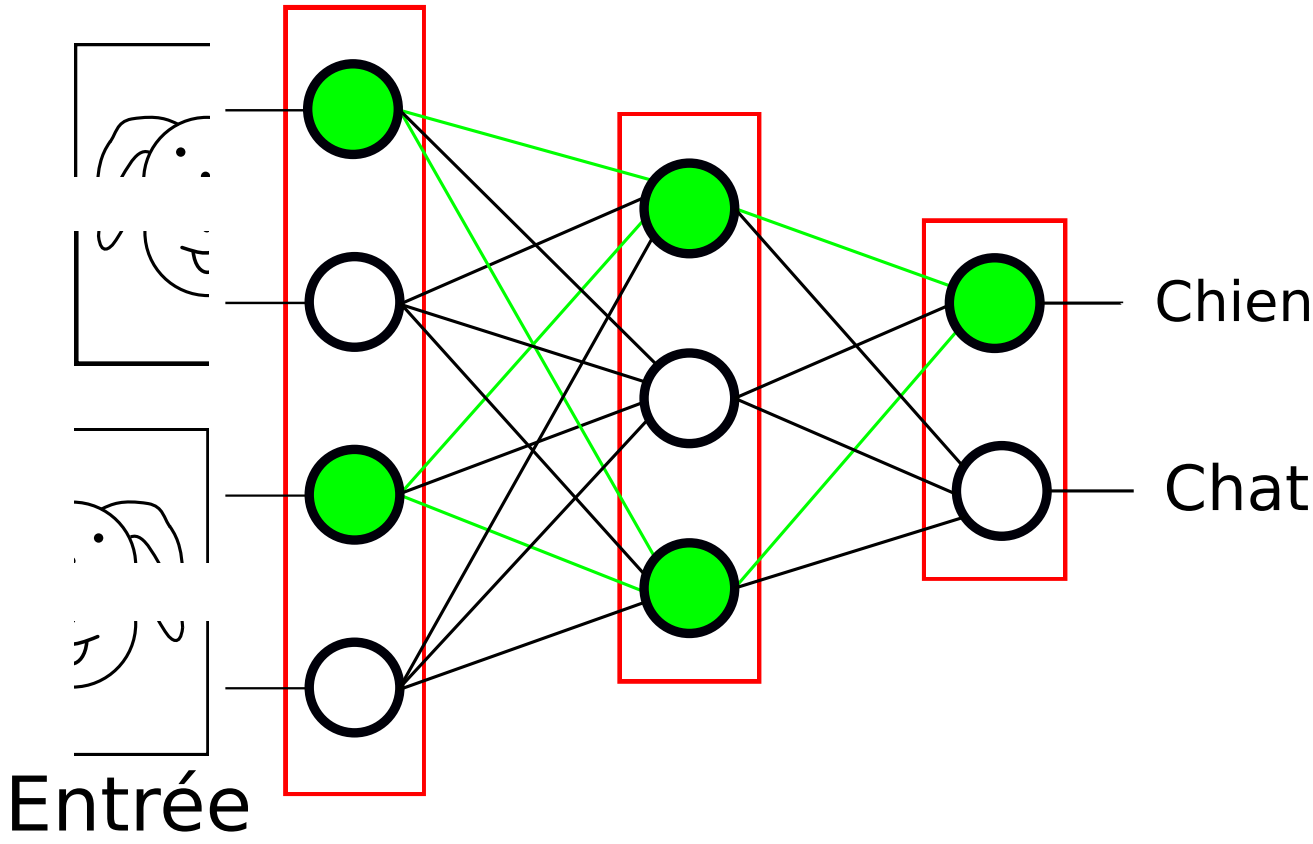
Exemple de réseaux de neurones (1)



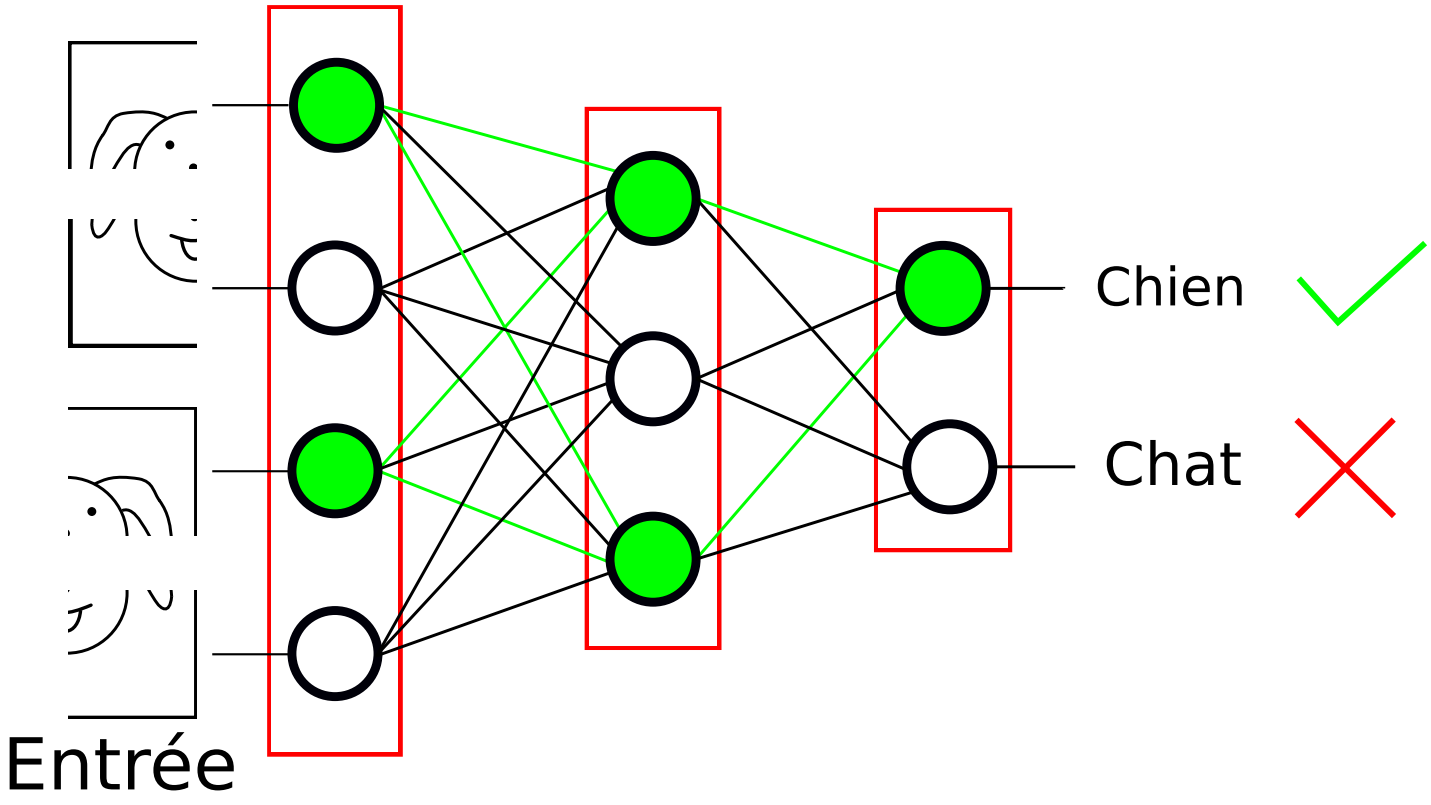
Exemple de réseaux de neurones (1)



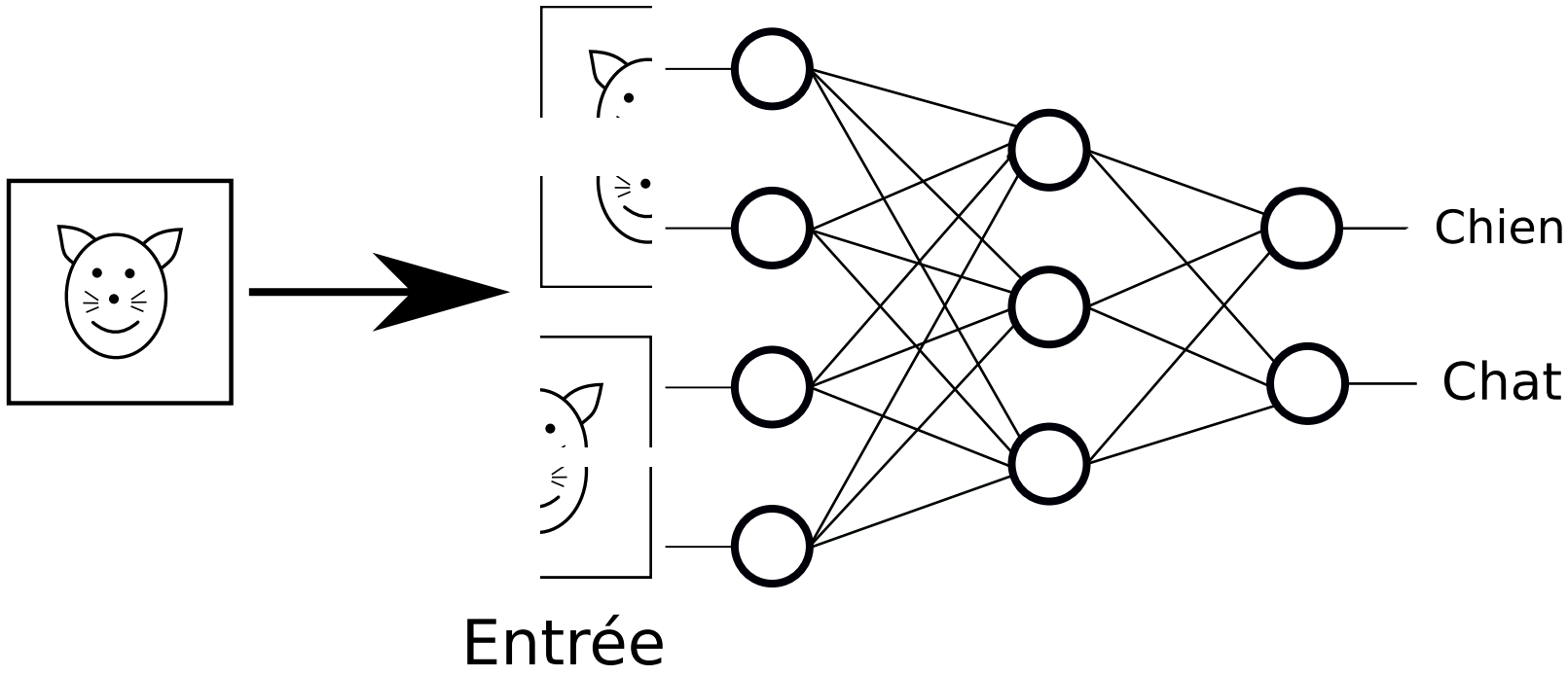
Exemple de réseaux de neurones (1)



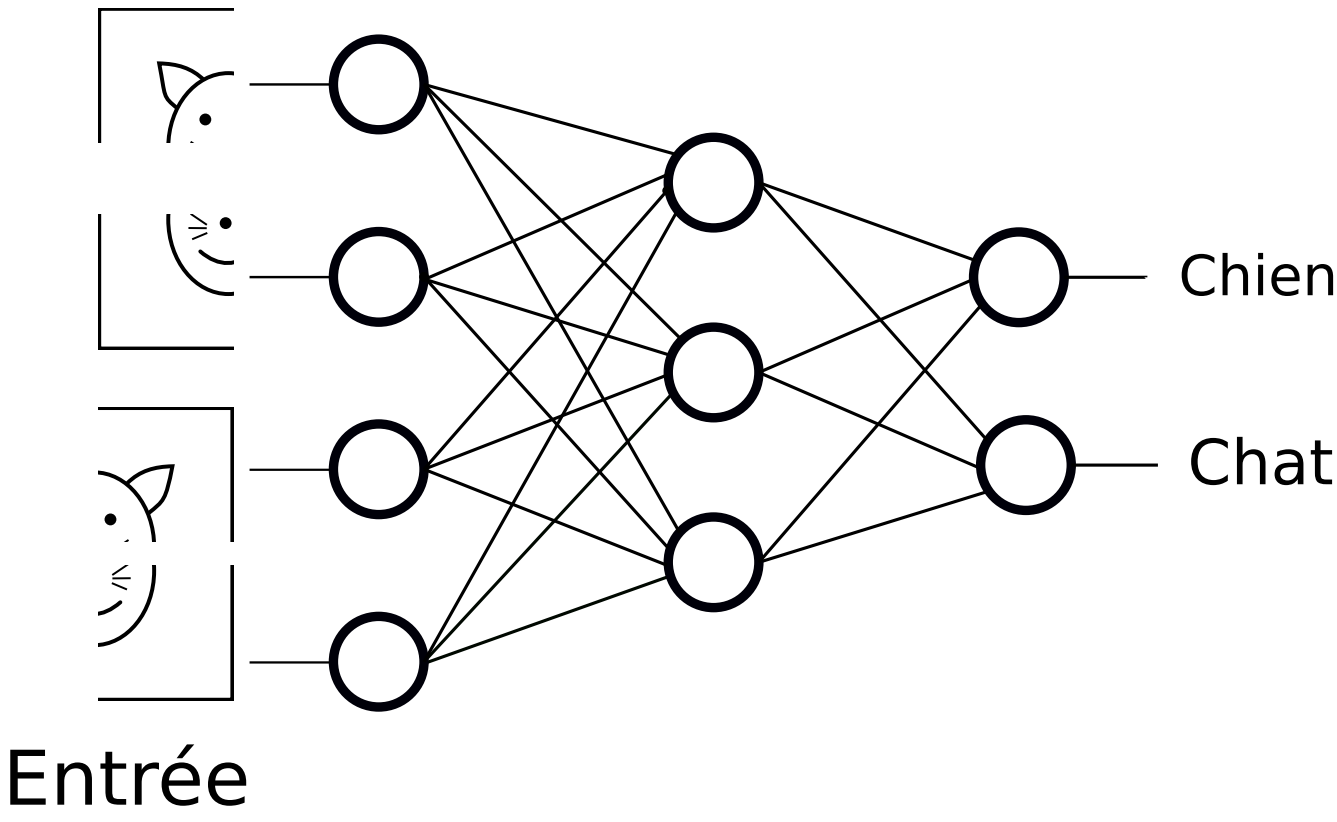
Exemple de réseaux de neurones (1)



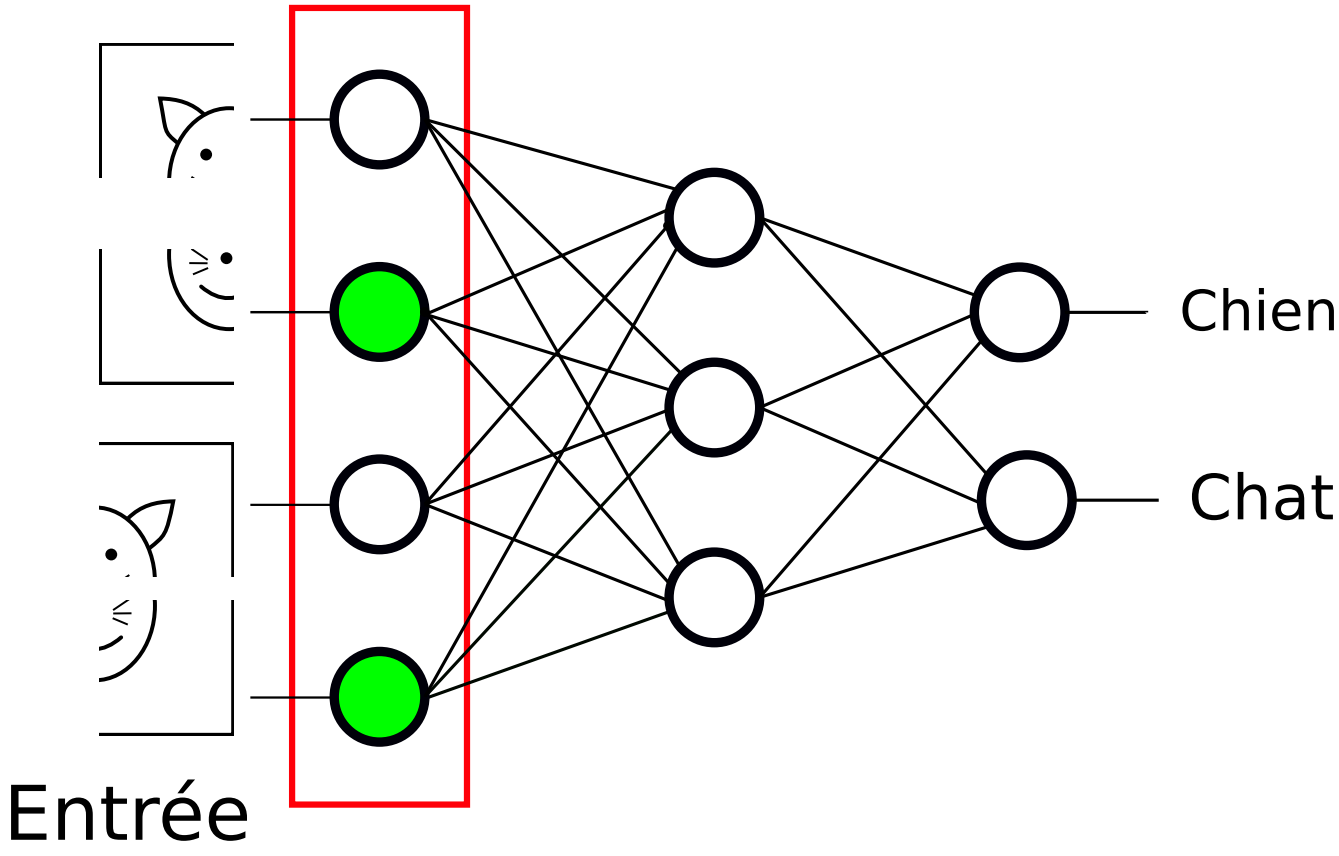
Exemple de réseaux de neurones (2)



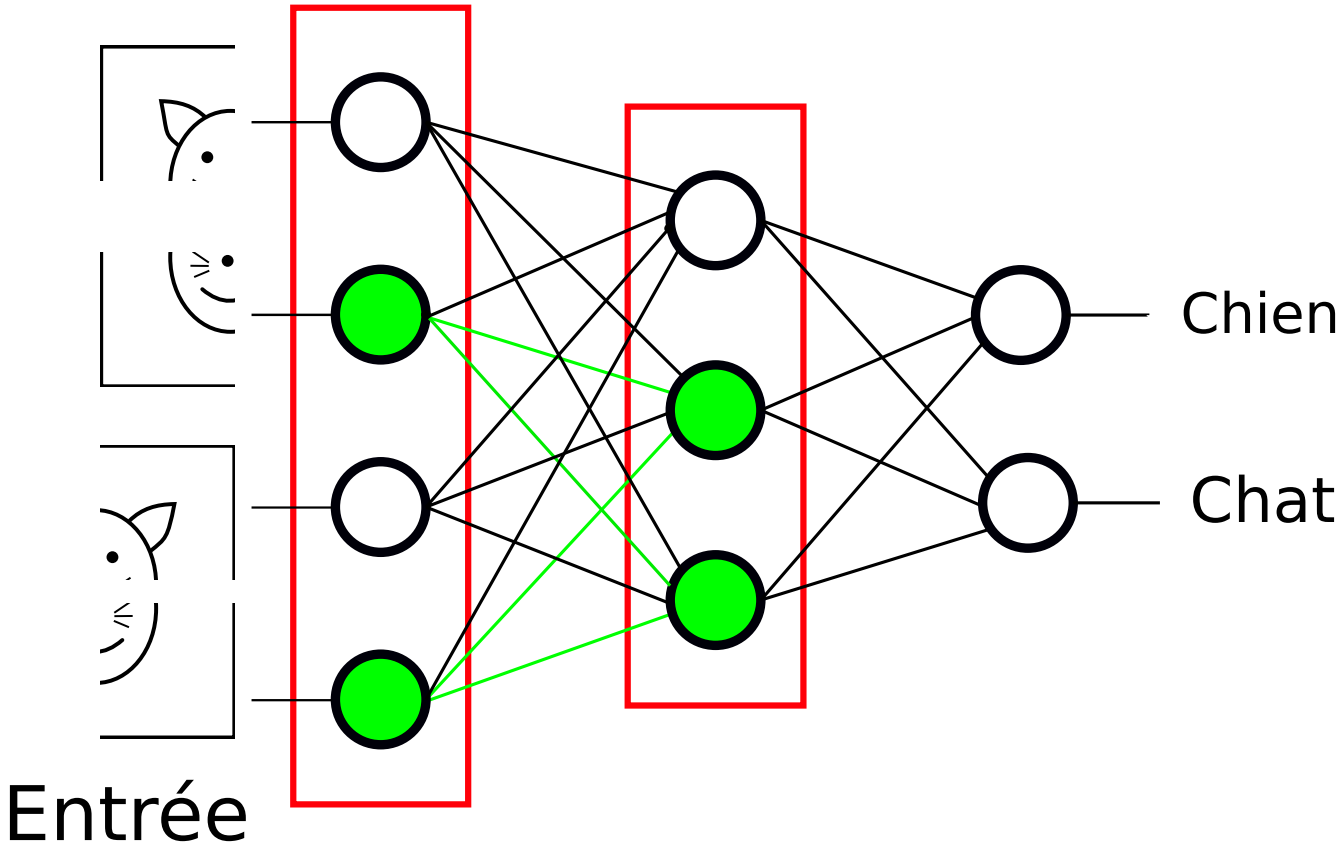
Exemple de réseaux de neurones (2)



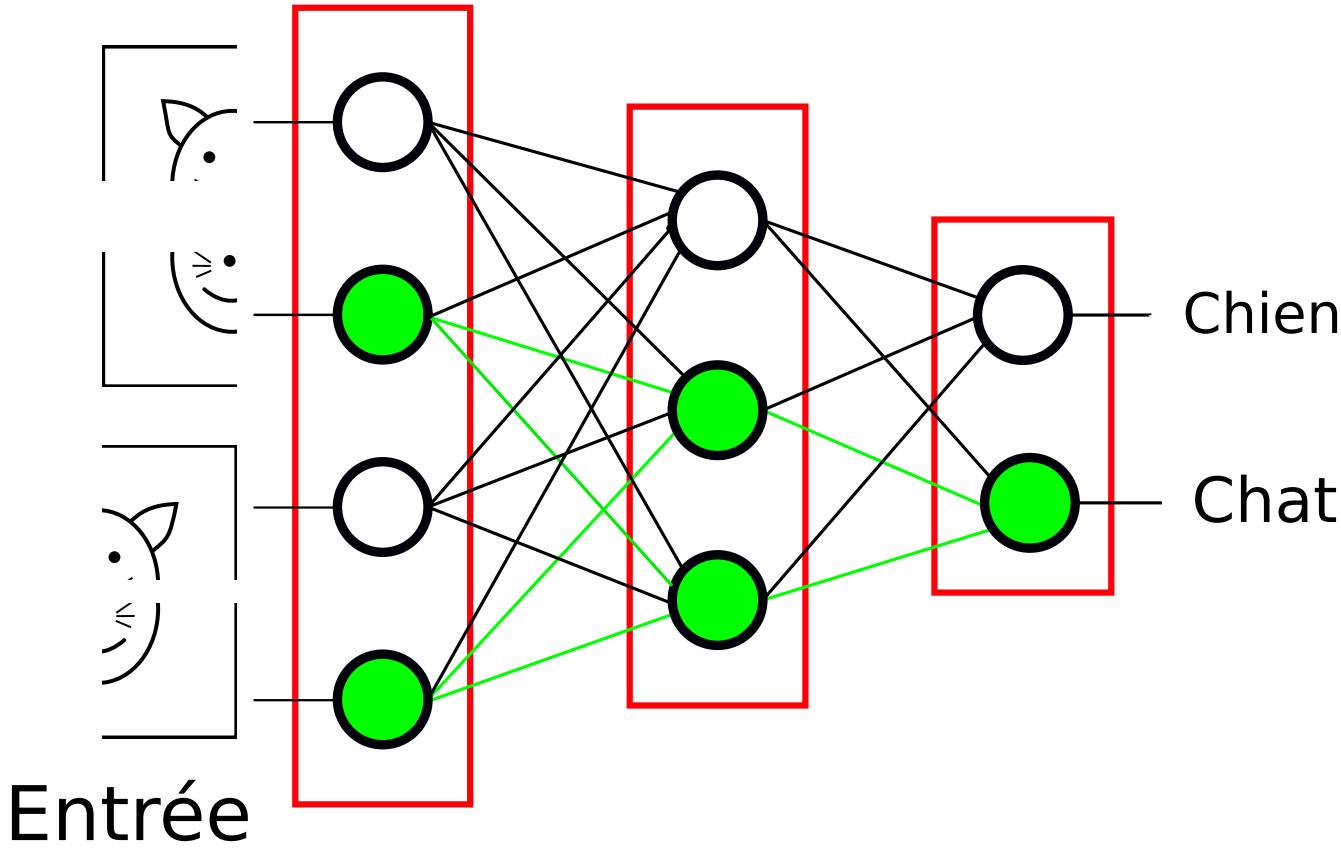
Exemple de réseaux de neurones (2)



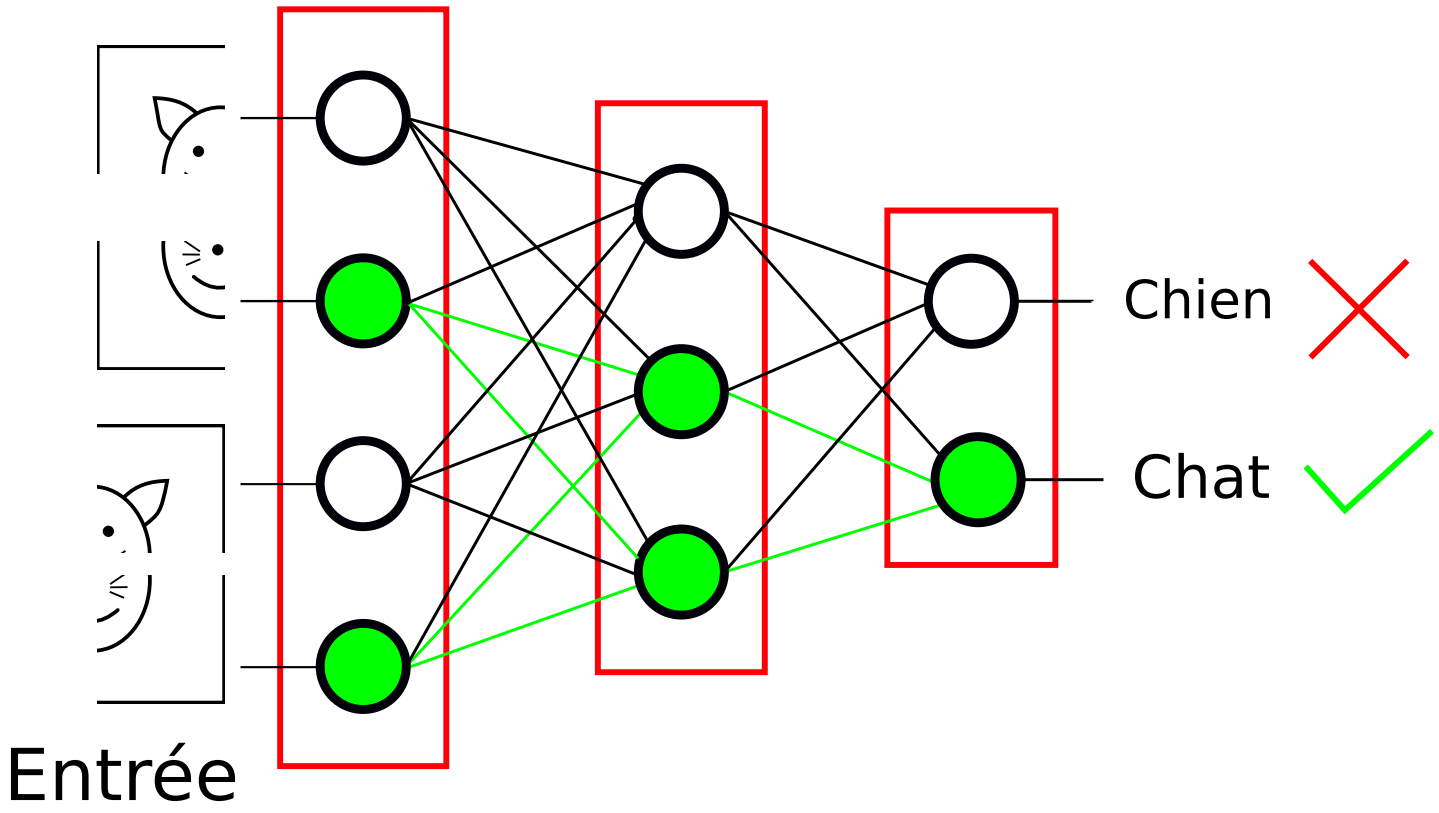
Exemple de réseaux de neurones (2)



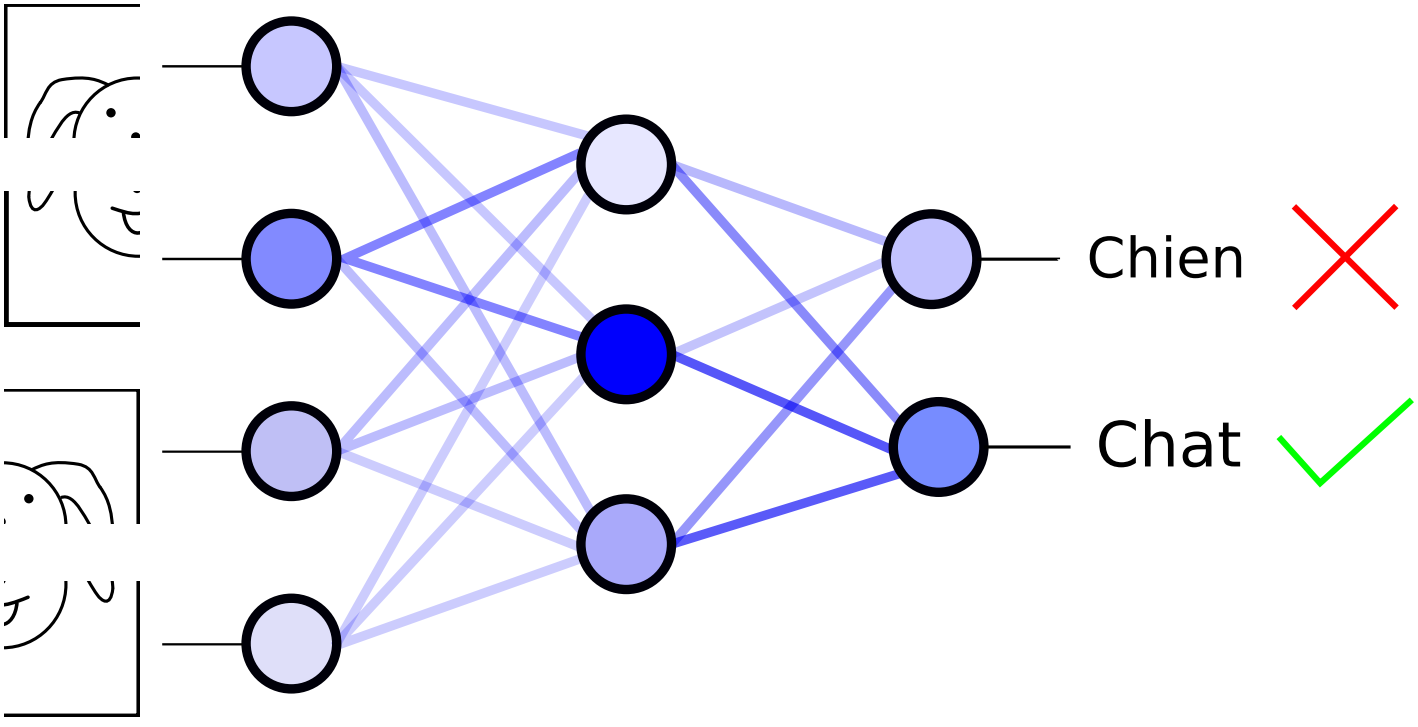
Exemple de réseaux de neurones (2)



Exemple de réseaux de neurones (2)

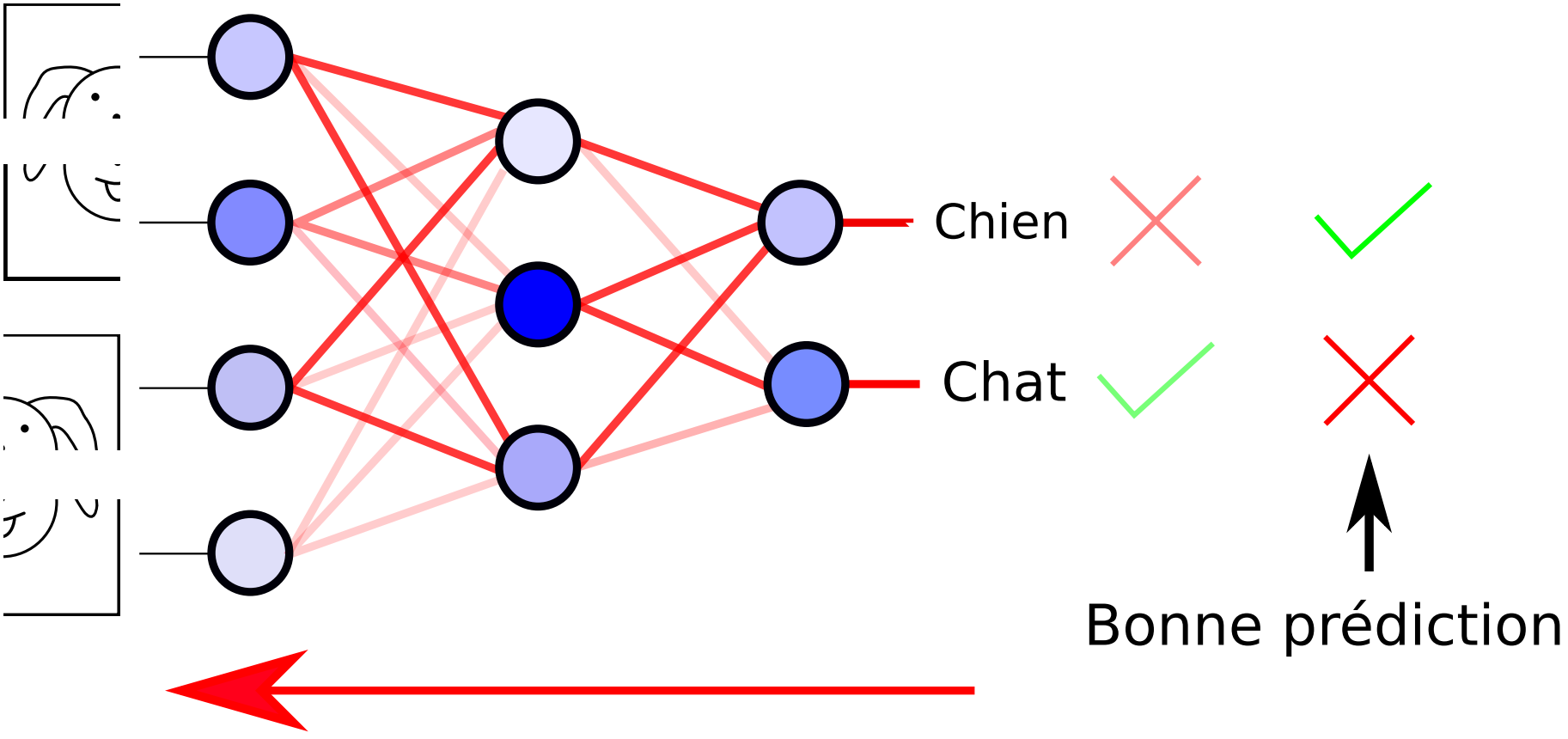


Comment un réseau fait-il pour apprendre ?



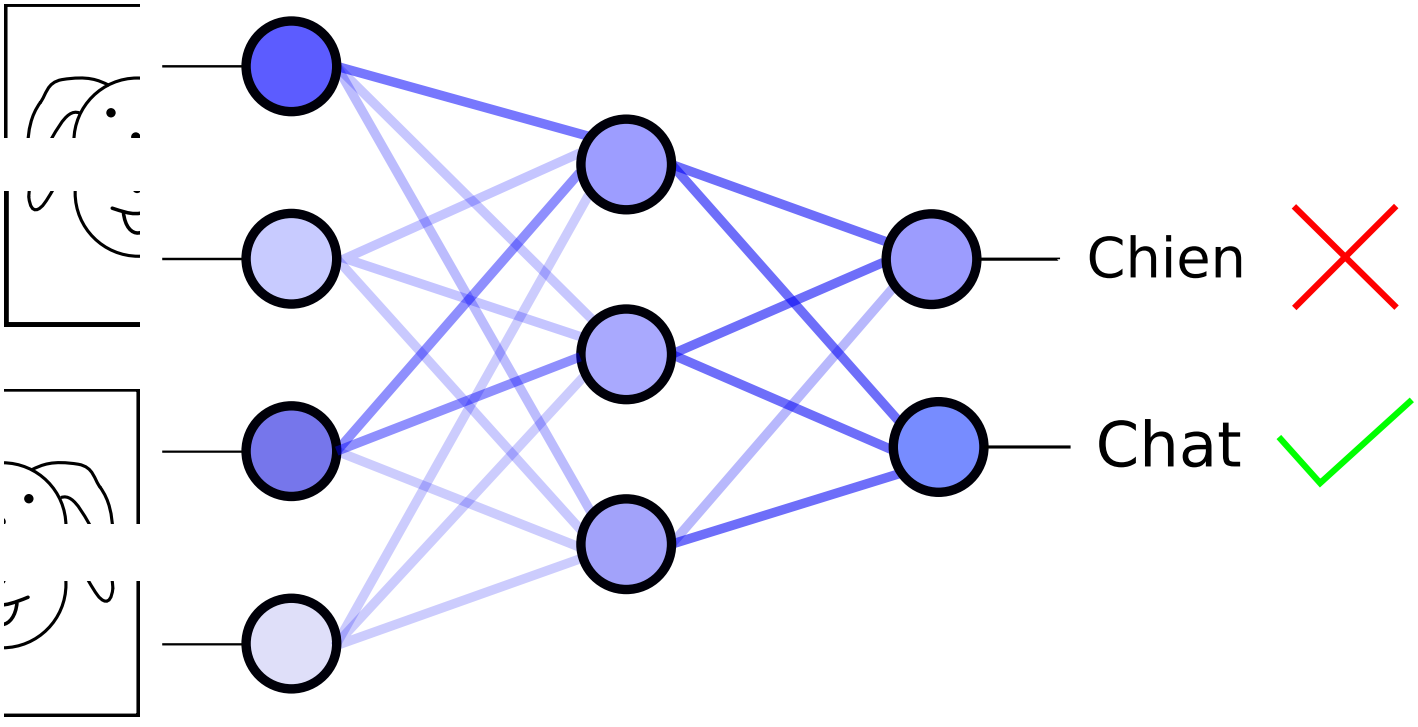
Prédiction du réseau

Comment un réseau fait-il pour apprendre ?



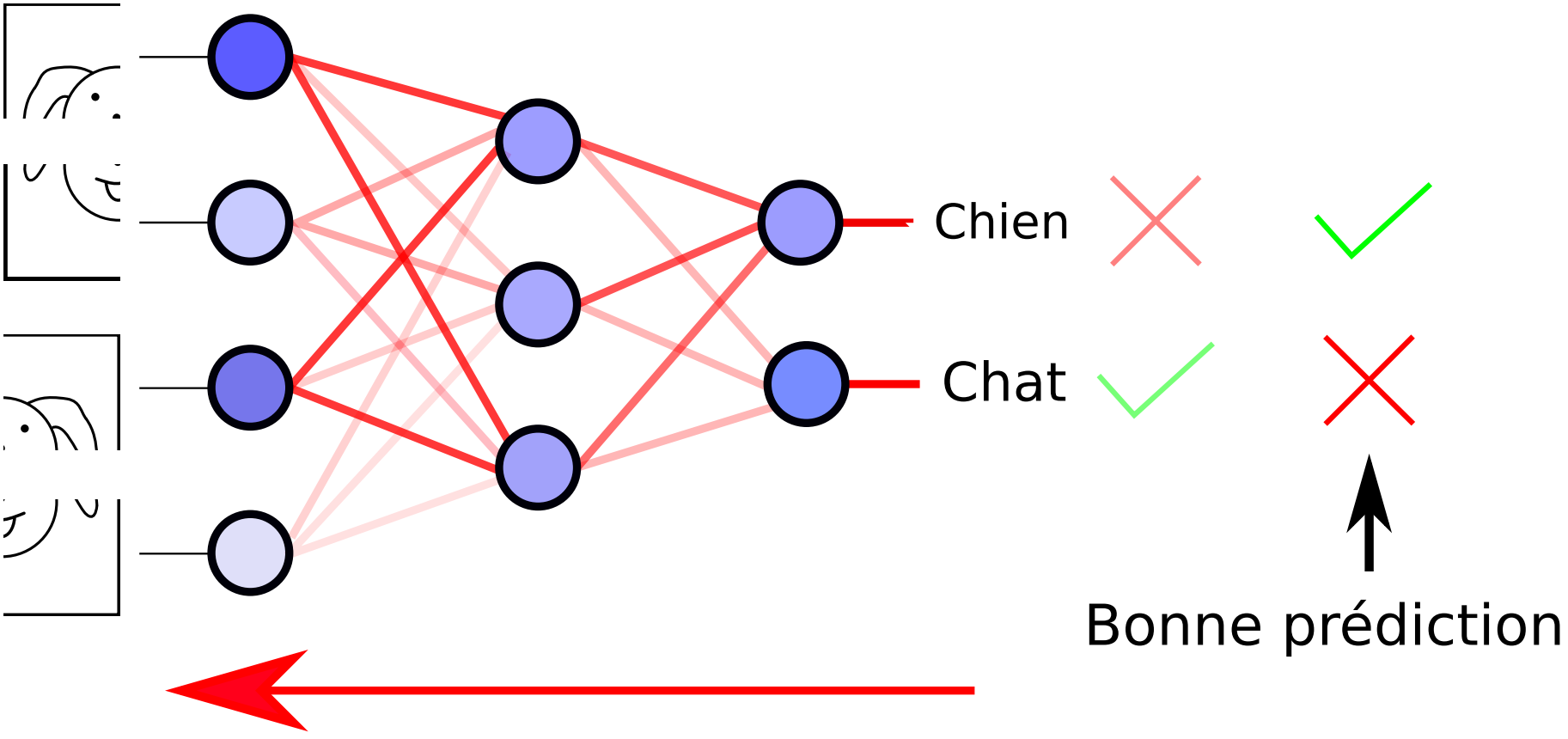
Correction grâce à la bonne prédiction

Comment un réseau fait-il pour apprendre ?



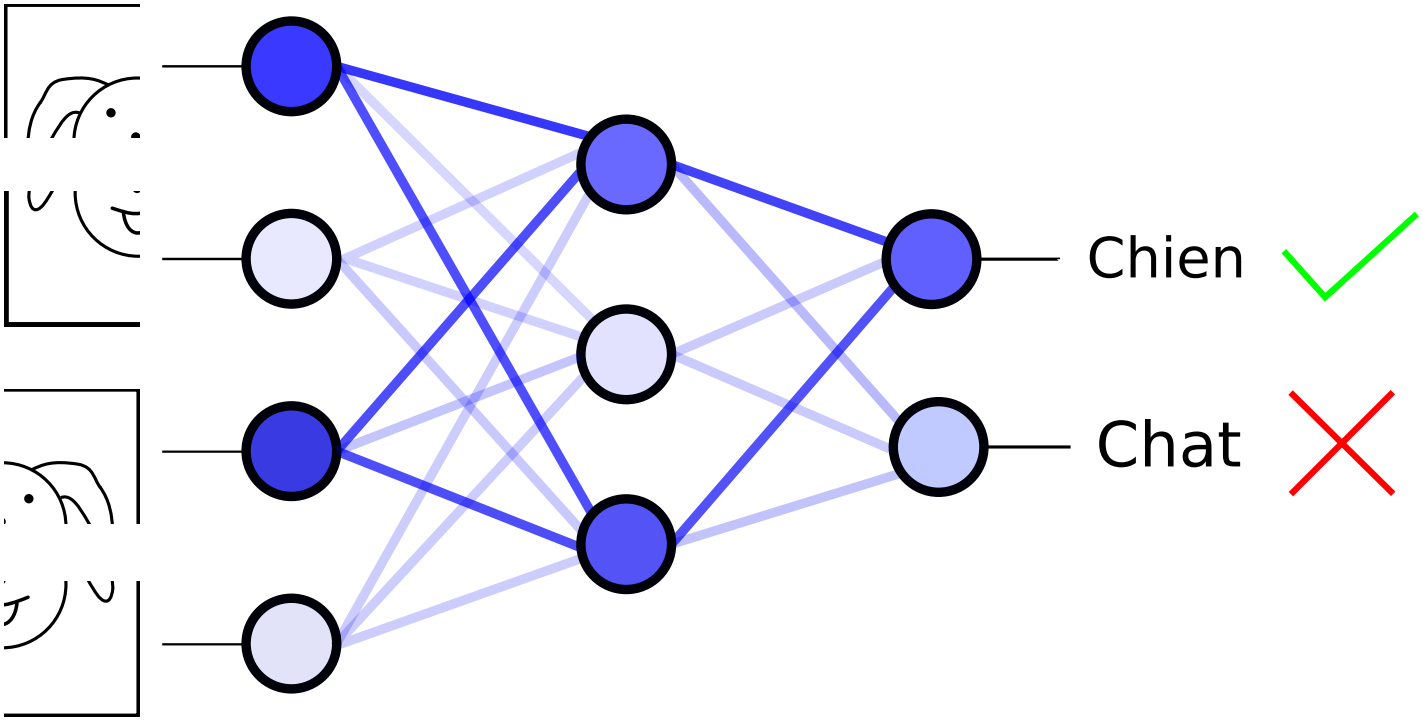
Prédiction du réseau

Comment un réseau fait-il pour apprendre ?



Correction grâce à la bonne prédiction

Comment un réseau fait-il pour apprendre ?



Prédiction du réseau

Retour à notre réseau

- Rappel des couches :
  - entrée : 500 neurones
  - 3 couches intermédiaires : 50 neurones chacunes
  - sortie : 256 neurones

Retour à notre réseau

- Rappel des couches :
  - entrée : 500 neurones
  - 3 couches intermédiaires : 50 neurones chacunes
  - sortie : 256 neurones

- Nombres de connexions à apprendre entre :
  - entrée & 1ère couche : $500 \times 50 = 25\,000$
  - chaque couche intermédiaire : $50 \times 50 = 2\,500$
  - dernière couche & sortie : $50 \times 256 = 12\,800$

Retour à notre réseau

- Rappel des couches :
  - entrée : 500 neurones
  - 3 couches intermédiaires : 50 neurones chacunes
  - sortie : 256 neurones

- Nombres de connexions à apprendre entre :
  - entrée & 1ère couche : $500 \times 50 = 25\,000$
  - chaque couche intermédiaire : $50 \times 50 = 2\,500$
  - dernière couche & sortie : $50 \times 256 = 12\,800$

- Nombre total :
  - → $25\,000 + 2\,500 + 2\,500 + 12\,800 =$ **42 800 connexions**

Merci pour votre attention

N’hésitez pas si vous avez des questions

Et bon courage pour le quizz …

Mais avant tout santé ! :-)

Quizz

Question 1

Que signifie le sigle AES ?

(A) Archeologic European Society

(B) Advanced Encryption Standard

(C) Analog Electromagnetic System

(D) Adequate Emission Sound

Question 2

Quel est l'ordre de grandeur de 2^{128} ?

(A) des milliards

(B) des milliards de milliards

(C) des milliards de milliards de milliards

(D) des milliards de milliards de milliards de milliards

Question 3

Qu’est ce qui caractérise la cryptographie symétrique ?

(A) Elle nécessite un miroir

(B) La clé de chiffrement sert aussi à déchiffrer

(C) Les messages sont indéchiffrables

(D) Elle est très peu utilisée

Question 4

Combien de bits y a-t-il dans un octet ?

(A) 8

(B) 9

(C) 10

(D) 11

Question 5

Quel est l’objet le plus sécurisé (en moyenne) ?

(A) Un badge de porte d’entrée

(B) Un ordinateur de bureau

(C) Une carte bancaire

(D) Un smartphone

Question 6

Qu'obtient-on en appliquant le chiffrement de César au message ‘‘PINT OF SCIENCE’’ avec la clé 6 ?

(A) UNSY TK XHNJSHJ

(B) WPUA VM ZJPLUJL

(C) VOTZ UL YIOKTIK

(D) ECNEICS FO TNIP

Question 7

Quelle couche du réseau réalise la prédiction ?

(A) la troisième

(B) la première

(C) la dernière

(D) la deuxième

Question 8

Qui a gagné le Prix Alan Turing (l'équivalent du prix Nobel d'informatique) en 2018 ?

(A) Bengio, Hinton et LeCun

(B) Griezmann, Mbappé et Pavard

(C) Rivest, Shamir et Adleman

(D) Athos, Porthos et Aramis

Question 9

Que signifie MLP en Machine Learning ?

(A) Multi Layer Perceptron

(B) Multi Layer Prediction

(C) My Little Pony

(D) Memory Level Parallelism

Question 10

Si mon réseau a 5 neurones en entrée, 5 neurones intermédiaires et 5 neurones en sortie, combien de connexions a-t-il à apprendre ?

(A) 550

(B) 50

(C) 42

(D) 15

Question Bonus

Pour qui travaillait Edward Snowden ?

(A) La CIA

(B) La NSA

(C) Le KGB

(D) La DGSI