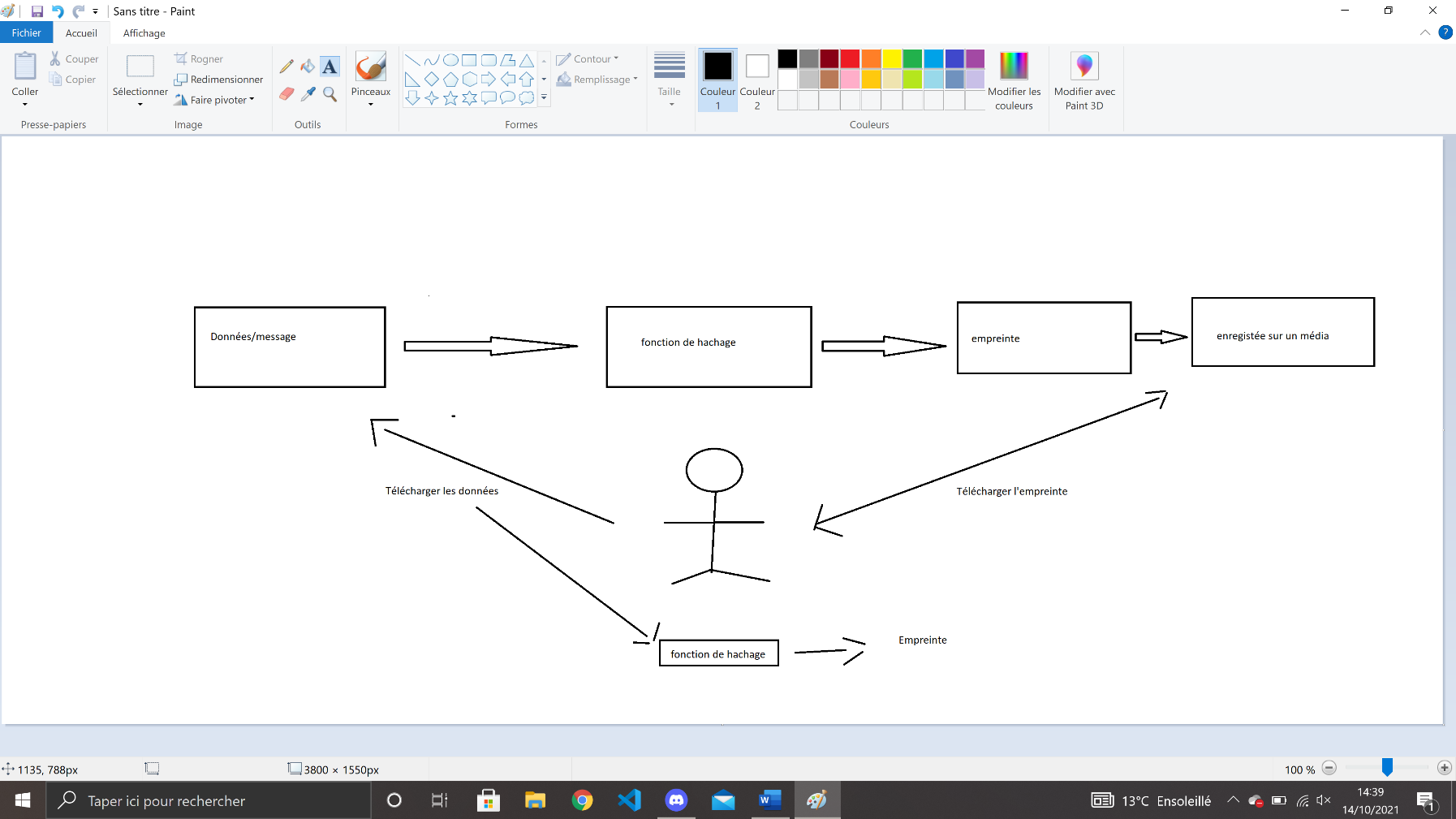
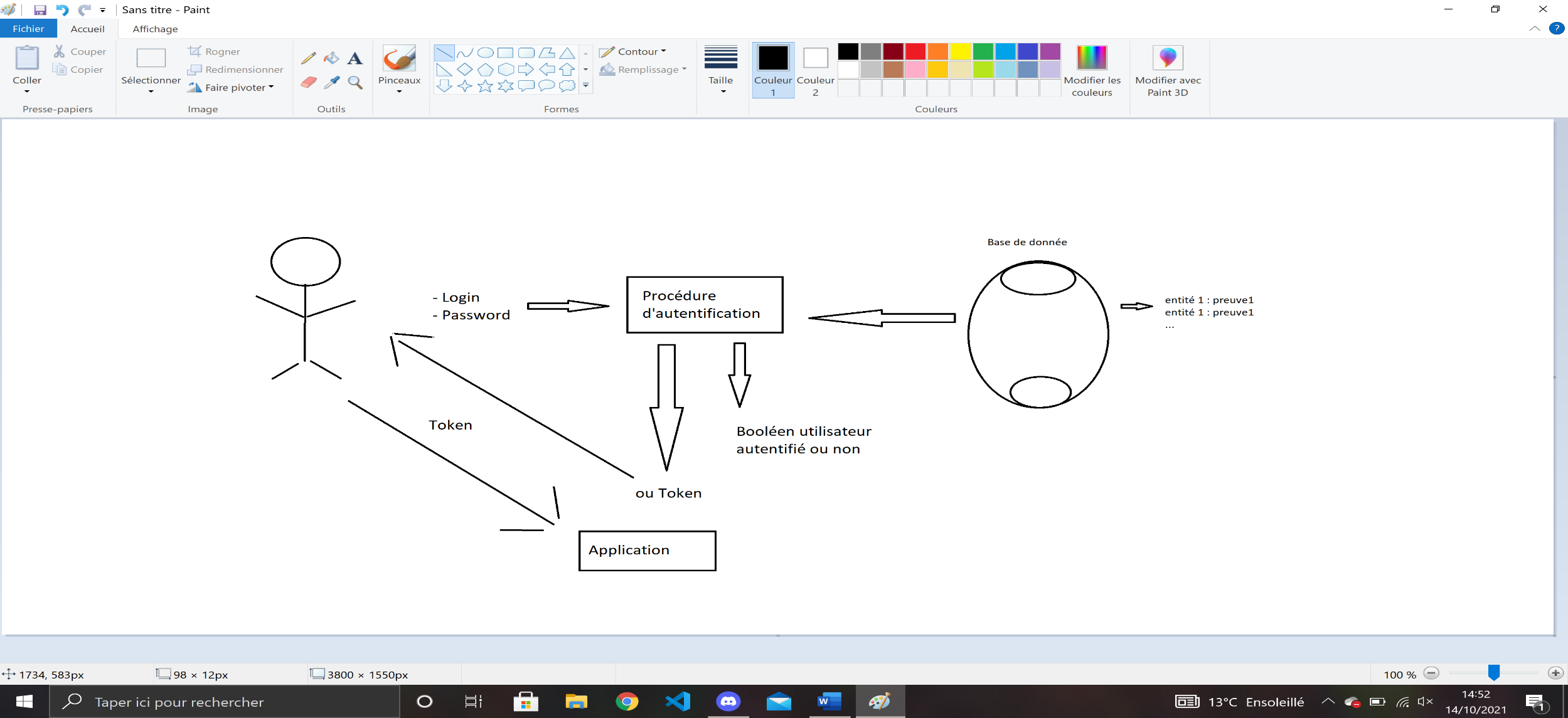
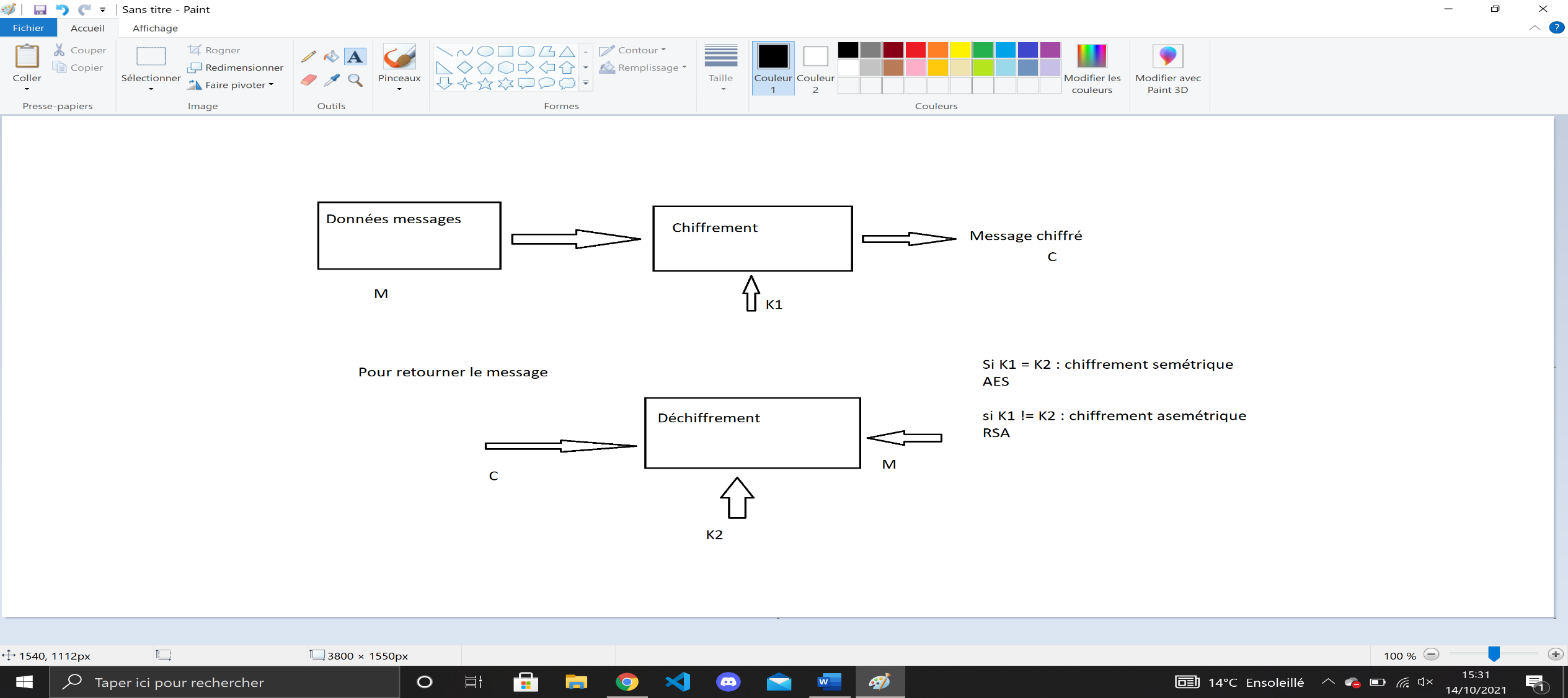
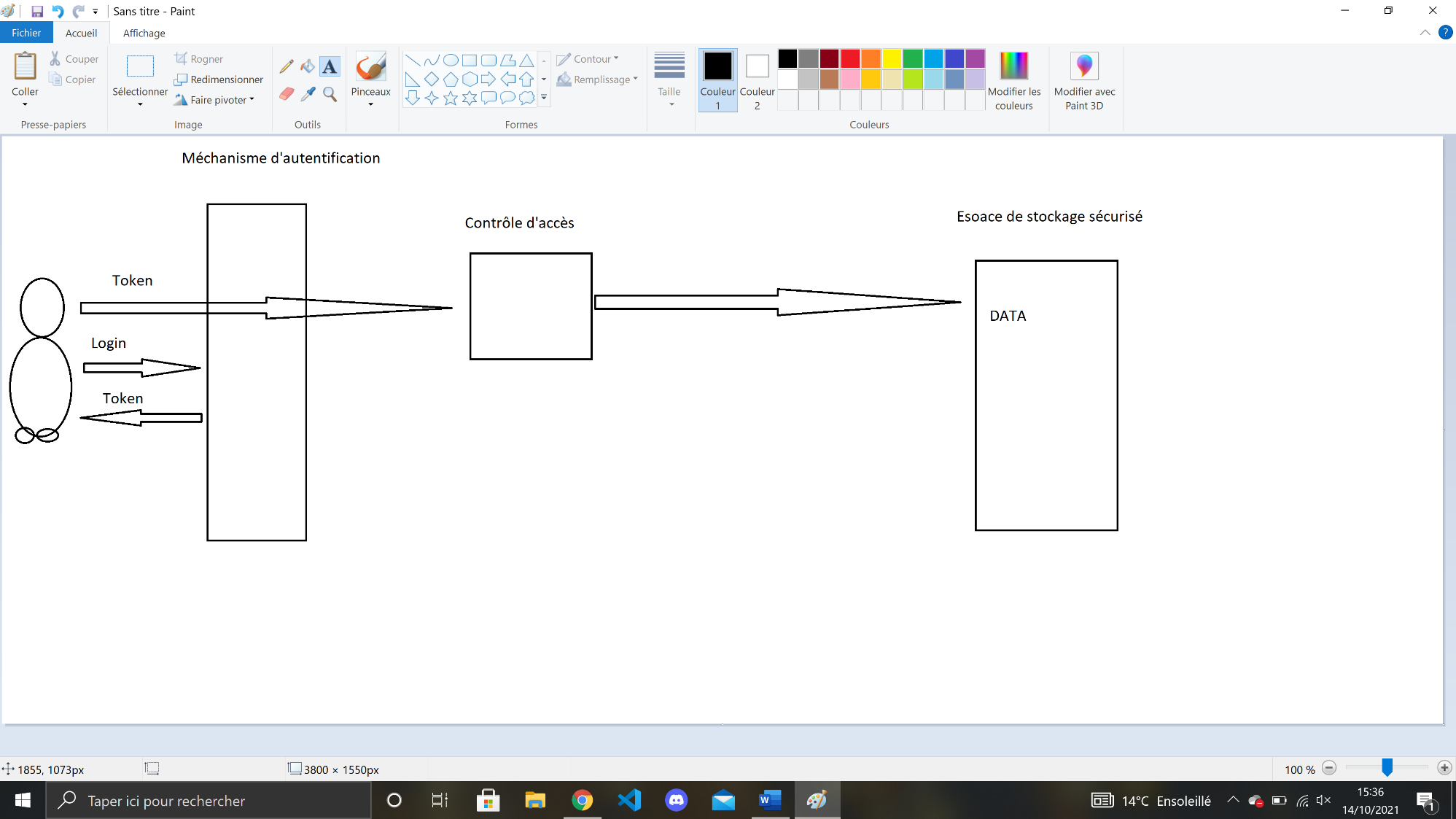
* Question 1
  + **Sécurité** : protection contre les menaces intensionnelles
  + **Sûreté** : protection contre les menaces non-intensionnelles
* Question 2
  + **Intégrité** : vérifier que des données émise/stockées n’ont pas été modifiées.
  + **Autentification** : s’assurer de l’identité d’une entité
    - **Autentification avec une base de données**:
    - **Authentification avec document infalsifiable :** le document fourni par l’entité ne peut pas avoir été généré par une autre entité différente de l’autorité administratif qu’il l’a délivré.
  + **Confidentialité** : martien du secret des informations.
    - **Chiffrement** :



* + - **Autre méthode pour confidentialité** : coffre-fort
      * **Authentification**
      * **Contrôle d’accès** (permission)
* Question 3 :
  + **Non-répudiation**: une entité ne peut pas nier qu’elle réalise une action. Elle ne fait pas intervenir ni de la confidentialité ni le contrôle d’accès, en revanche, elle nécessite de l’authentification et de l’intégrité.
* Question 4 :
  + Disponibilité de 99.9% -> indisponibilité de 0.1%.
  + Temps d’indisponibilité par an : 365 \* 24 \* 0.001 = 8.7h
  + 1ère raison d’indisponibilité :
    - Maintenance (mis à jour système et fimware-bios)
  + 2ème raison d’indisponibilité :
    - Erreur de manipulation
* Question 6 :
  + Sécurité web d’une entreprise :
    - Disponibilité : très fort
    - Intégrité : très fort
    - Confidentialité : faible ou aucune
    - Traçabilité : faible (sauf dans le cas d’obligation légale, réquisition juridique )
* Question 7 :
  + Page 6
  + Active directory ou LDAP --> sécurité logique
* Question 8 :
  + Fermeture clé de la salle serveur 🡪 sécurité physique
* Question 9 :
  + Règlement générale pour la protection des données (données personnelles :données associées à une personne)
  + Obligation définis dans RGPD :
    - Consentement de la personne sur laquelle on va stocker des informations
    - Droit à l’oublie
    - Portabilité des données
    - Information des utilisateurs en cas de fuite de données
  + Sanctions : 20.10^6 € ou 4% du chiffre d’affaires annuel
* Question 10 :
  + C’est un document écrit d’une soixantaine de page qui formalise l’importance donnée à la sécurité du système d’information de l’entreprise.
  + Document rédigé par les hautes instances de l’entreprise
* Question 11 :
  + Tous les employés de l’entreprise.
* Question 12 :
  + Utilisation résiduelle
* Question 13 :
  + Plan de reprise (continuité) d’activité définit les manipulations, les procédures à effectuer en cas de perte d’un service.
* Question 14 :
  + L’élément d’une entreprise le plus difficile à sécuriser : l’élément humain.
  + La sécurité est plus importante que la tâche à effectuer
  + Les employés sont payés pour remplir une tâche, assez souvent en un temps limité.
  + Le premier objectif de l’employer est de faire ce pourquoi il est payé. Or assez souvent, le respect des règles de sécurité risque de lui imposer d’arrêter de faire son travail, l’employé est en face à un dilemme :
    - Effectuer son travail
    - Ou respecter les règles de sécurité.
  + La décision d’arrêter son travail n’est pas facile à prendre
  + Comment améliorer l’élément humain :
    - Formation :
      * Lorsque l’employé arrive dans l’entreprise
      * Périodique pour rafraîchir et tenir compte de l’évolution.
      * Formation concrète, très proche de métier de l’utilisateur formé
      * Mais aussi suffisant générale pour que l’employé puisse prendre des décisions en autonomie lorsqu’il est face à un nouveau problème.
* Question 16 :
  + Attaque APT (Advanced Persistent Threat) : l’attaquant à accès pendant une grande durée aux SI
* Question 17 :
  + Attaque DOS (Denial of service) : déni de service
    - Objectif : rendre indisponible un service
    - Comment :
      * Saturation de ressources (mémoire, CPU, …) du système attaqué.
      * Saturation du réseau auquel est connecté le système.
    - Pour surcharger les ressources, le pirate envoie des demande connexion TCP. à chaque demande de connexion TCP, de la mémoire est réservé pour conserver les paramètres de la connexion, si on reçoit beaucoup de demandes de connexion, la mémoire de système peut être surchargé.
    - Pour surcharger le réseau, le pirate envoie une requête simple à un serveur B qui renvoie une grande réponse et changeant l’adresse IP du pirate à l’adresse du serveur ciblé A, comme ça le serveur B envoie la grande réponse au serveur A grâce à la petit requête envoyée par le pirate (ça traite la différance entre les ports passant du pirate et celui du serveur ciblé)
  + Attaque D DOS (Distributed Denial of service)
    - Toujours un grand sujet d’étude académique pour contrer ces attaques.
    - Au lieu que l’attaque soit menée à partit d’une seule machine, elle va être déclenchée par plusieurs machines (objets connectés) piratées dont le pirate à pris le contrôle, donc difficile de distinguer les demandes légitimes avec les demandes pas légitimes.
* Question 18 :
  + Social Engineering 🡪 cible : élément humain, employés de l’entreprise : Fishing
* Question 19,20 :
  + Bof…ui
* Question 21 :
  + Relire la parte sécurité application page 6
  + Partie audit page 19 & 20
  + Failles de sécurité liées au dev d’applications :
    - Buffer overflow
    - SQC injection
    - CSRF
    - XSS
  + Moyen de prévention :
    - Security development lifecycle (les bonnes pratiques pour le développement sécurisé)
    - Revu de code orienté sécurisé
    - Analyse statice du code
    - Les testes
* Question 22 :
  + Pare-feu
    - Rôle : filtrer des paquets, il va permettre d’autoriser des connexions vers des services.
    - DMZ : zone démilitarisée. C’est de mettre tous les serveurs accessible depuis l’extérieurs dans une seule zone qu’on appelle (DMZ), afin de limiter les dommages au cas d’attaque depuis l’extérieur. Et protéger les serveurs internes