Lundi 4 avril :

- Arrivée vers 9h20

- Visite et présentation avec Sébastien Canard

- Remise des documents ainsi que le badge

- Documents comprenants :

- Plan d'évacuation

- Fiche accueil à remplir avec Loïc demain

- Fiche prévention et qualité de vie au travail

- Fiche avec identifiants et mdp pour connexion session ordi

- Article "Let's talk about ZRTP"

- Photos imprimées qui sont dans l'article

- Article "ProVerif Analysis of the ZRTP Protocol"

- Étude du premier article sur le protocole ZRTP, compréhension du fonctionnement

- Pause vers 10h30 et reprise vers 10h45

- Poursuite d'étude du premier article et fin vers 12h

- Pause repas 12h-13h30 et jungle speed (bonne intégration à l'équipe des stagiaires)

- Reprise avec étude du deuxième article sur ZRTP

- Fin vers 15h

- Tentative d'installation d'Android Studio mais problème de droit

- 15h30 : lecture d'autres articles sur ZRTP sur le net et de BZRTP

- 16h40 : Nouvelle tentative d'installation avec découverte d'Adminute

- 17h : Android Studio installé mais problème avec le SDK car proxy bloquant

- 17h10 : Recherche de solutions, conclusion : Installation des SDK à la maison

- 17h30 : Rédaction du journal de bord

- Départ vers 17h50

Mardi 5 avril :

- Arrivée vers 7h45

- Mise en place de l'environnement de travail

- Tentative de faire fonctionner Android Studio

- Firewall du Wi-Fi bloque le téléchargement même en admin

- Passage sur connexion personnelle

- Construction assez longue

- Problème de création de device : Problème de connexion une nouvelle fois

- Application de base avec juste Hello World fonctionne !

- Réunion d'information avec le tuteur de stage : Loïc Ferreira

- Présentation du protocle ZRTP plus en détail

- Explication de la mission du stage :

- Dans un premier temps, obtenir un protocol ZRTP qui compile et qu fonctionne entre deux terminaux

- Puis essayer de réaliser un échange entre deux émulations de téléphone via Android Studio avec numérisation de voix (regarder Linphone)

- Suite à cela, réaliser la partie optionnel de signature avec algorithme classique tel que le RSA puis avec crypto post-quantique (Biblio telle que OQS et pqClean)

- Enfin ajouter dans l'échange de clef DH un envoi de clef avec algorithme post-quantique

- Demande de matériel en fin de réunion

- Installation de l'environnement afin de regarder l'implémentation de BZRTP

- Installation de WSL2

- Installation de code

- Réception d'un nouveau clavier

- Pause déjeuner entre 12h et 13h30

- Reprise avec étude de BZRTP qui ne compile pas dans un premier temps

- Installation de CMAKE sous WSL puis beaucoup de tentatives de compilation sans succès

- Réunion d'accueil des RH de 15h à 16h

- Départ vers 16h15

Mercredi 6 avril :

- Arrivée vers 7h45

- Réception du matériel commandé

- Mise en place du bureau

- Tentative de compilation avec quelques avancées mais problème toujours avec multiples téléchargements

- Installation de CMAKE sous Windows

- Inutile car cela ne fonctionne pas comme prévu

- Tentative de résolution de CMAKE sur bctoolbox

- Téléchargement et compilation de BcUnit sans trop de problème

- Pause du midi entre 12h et 13h30

- Téléchargement de la bibliothèque mbedtls et compilation sans problème

- Suppression de certaines options de sorte à ce que le CMAKE fonctionne

- Le CMAKE fonctionne

- Tentative de CMAKE sur bzrtp

- Pour l'instant infructueuse mais poursuite d'étude

- Il faut espérer que les options enlevées dans bctoolbox n'ont pas d'impact sur bctoolbox dans bzrtp

- Départ vers 16h15

Jeudi 7 avril :

- Arrivée vers 7h45

- CMAKE réussi sur BZRTP après avoir à peu près compris comment ça fonctionnait

- Documentation sur le code, avoir une idée de son utilisation

- Tentative d'inclure la bibliothèque externe dans un programme qui l'utiliserait

- Conférence sur la 5G entre 10h et 11h10

- Tentative d'inclusion à nouveau avec un peu de progrès mais pas trop

- Pause repas entre 12 et 13h30

- Reprise des tentatives d'inclusion avec plus ou moins réussite car problème de compilation de l'inclusion, à retravailler demain et à comprendre

- Départ vers 16h00

Vendredi 8 avril :

- Arrivée vers 7h30

- Étude de la librairie BZRTP afin de mieux en comprendre le fonctionnement

- Reprise des tentatives d'inclusion avec assez peu de succès mise à part la libération de tous les blocs mémoires

- Pause repas entre 12h et 13h30

- Étude de l'application Linphone afin de comprendre où l'inclusion était

- Reprise des tentatives d'inclusion avec modification de fonctions pour savoir si on prend bien tout en compte, problème avec isInitialised qui reste à 0

- Départ vers 16h

Lundi 11 avril :

- Arrivée vers 7h40

- Reprise des tentatives d'inclusion

- Étude de l'application Linphone à nouveau, avec pour but de trouver l'endroit où bzrtp est utilisé, ce qui n'a toujours pas été trouvé

- Requête à ne pas oublier pour compiler : ./autogen.sh && ./configure && make && sudo make install

- Contact avec monsieur Loïc Yon, afin d'obtenir un peu d'aide sur la compilation et inclusion de bibliothèque

- Pause repas entre 12h et 13h30

- Reprise avec l'étude de Linphone, toujours pas concluante car la source n'a pas été trouvée

- Étude des inclusions dans le Makefile pour voir si tout est bien fait

- Compilation ok mais toujours problème avec les variables et les fonctions qui ne sont pas correctement appelées

- Départ vers 16h

Mardi 12 avril :

- Arrivée vers 7h45

- Compilation ok, fonctionnement ok mais je ne sais pas par quelle magie cela est possible. Les variables sont bien initialisées et la modification des fonctions de la librairie ont bien un effet

- Remerciement vers monsieur Yon

- Réunion avec Loïc de 10h à 10h40, présentation de l'avancée du travail, discussion autour du travail à faire

- Étude de mininet pour faire des petits réseaux et voir si des appareils peuvent établir un protocole ZRTP ensemble

- Étude afin de savoir comment fonctionne les premiers appels afin d'envoyer les messages Hello

- Pause repas entre 12h et 13h30

- Reprise avec étude de la fonction startChannelEngine, compréhension des appels et des sous-fonctions

- Étude du type bzrtpStateMachine qui est un pointeur vers une fonction qui prend en argument un bzrtpEvent\_t et renvoie un int

- Compréhension difficile de la fonction

- Tests réalisés et ok, la fonction state\_discovery\_init tourne, lorsque l'on met le type d'événement dans l'event, alors la fonction continue de tourner et veut que l'on initialise, renvoie l'erreur message innatendu si type est message à la place

- Renvoie bien 0 avec le INIT

- Départ vers 16h

Mercredi 13 avril :

- Arrivée vers 7h40

- Reprise des tests afin de comprendre les fonctions et de savoir comment s'en servir

- HelloPacket initialisé lorsque l'on initialise le channel

- Nombre d'algorthimes supportés à 2, pourquoi ? Modification dans la librairie bzrtp

- Problème avec KeyAgreement, il faut regarder si on a accès aux outils bctoolbox et identifier les fonctions qui correspondent TODO (cryptoUtils.c)

- Pause repas entre 12h et 13h30

- Étude afin d'envoyer le paquet vers Bob

- Une fois le paquet reçu, on utilisera la fonction processMessage afin de traiter le paquet reçu

- Départ vers 16h15

Jeudi 14 avril :

- Arrivée vers 7h40

- Reprise des essais d'envoi

- Problème avec la fonction sendData

- Pause repas entre 12h et 13h30

- Problème avec la même fonction qui est initialisée à NULL, est-ce vraiment le problème ?

- Départ vers 16h15

Vendredi 15 avril :

- Arrivée vers 7h40

- Reprise de la découverte de la fonction sendData et tentative d'implémentation de la fonction

- Problème sur comment modifier le void \*

- Pause repas entre 12h et 13h30

- Reprise sur la fonction sendData ... Toujours pas fonctionnelle

- Renseignement sur la fonction et ce qu'elle doit faire

- Peu de doc sur la fonction et son fonctionnement

- Départ vers 16h

Mardi 19 avril :

- Arrivée vers 7h40

- Reprise avec la fonction sendData

- Toujours pas ok, on n’accède pas à l'info qu'on veut

- Documentation du type void \*, fonctionnement assez clair

- Pause repas entre 12h et 13h30

- Problème de passage par valeur au lieu de par addresse

- Même comme ça problème d'accès aux valeurs, à voir où on se trouve dans l'architecture

- Départ vers 16h15

Mercredi 20 avril :

- Arrivée vers 9h15

- Étude de l'architecture et des étapes à faire pour envoyer le paquet

- Vérification de compréhension de ce qu'il y a à faire

- Incompréhension dans la fonction init : lorsque l'on reçoit un message, on appelle init, si HelloMessage alors on répond avec un Ack (jusque là ok) et après on attend un Ack mais pourquoi on ne dit pas en même temps qu'on envoie le HelloPacket ?

- Fonction sendData a pour but de stocker dans le clientData du receveur le paquet qu'on envoie donc on doit reconstruire le paquet

- Fonction partiellement réussie

- Départ vers 17h30

Jeudi 21 avril :

- Arrivée vers 7h40

- Fonction sendData problématique pour la gestion de mémoire

- Problème de libération

- Problème aussi de gestion de données, dans waitingForHello, on appelle deux fois la fonction sendData ce qui fait que clientData est écrasée avant de pouvoir traiter

- Passer clientData sous forme de liste pour mieux gérer le tout

- Pause repas entre 12h et 13h30

- Écriture des différents problèmes et schématisation du protocole

- Réunion avec Loïc de 14h30 à 15h30

- Problème résolu grâce à une utilisation d'une liste de variable globale (plus tard à mettre dans le clientContext)

- Commencement de la mise en place

- Départ vers 16h

Vendredi 22 avril :

- Arrivée vers 9h10

- Mise en place des listes en variable globale, fonctionnement ok

- On continue le processus de développement

- Dans la queue de Bob, on va traiter le Ack d'Alice afin d'envoyer le commit de Bob

- Ensuite on continue de traiter le commit de Bob par Alice

- Pause repas entre 12h et 13h30

- Mise en place de la partie d'échange

- Problème avec le sequenceNumber

- On crée à nouveau le message Commit pour mettre à jour le sequenceNumber

- On obtient les DHPart en mettant à jour le nombre de séquence de Bob à chaque fois (ce qu'il faut faire au lieu de créer un paquet)

- Départ vers 17h

Lundi 25 avril :

- Arrivée vers 7h40

- Problème dans le programme, abouti au bout résultat pas tout le temps

- Moyenne de presque un sur deux

- Fouille dans le programme pour savoir où ça se passe

- Je pense à une erreur dans l'ajout dans la file de packet

- Mais ça vient pas de là

- Pause repas entre 12h et 13h30

- Reprise en cherchant toujours le problème

- Problème trouvé : comparaison du HVI

- Personne est responder et c'est un problème à gérer

- Comment faire ?

- Je regarde dans les différents protocoles que j'ai

- Départ vers 16h

Mardi 26 avril :

- Arrivée vers 9h

- Résolution du problème de comparaison de HVI

- Si Alice n'a pas envoyé le DHPart 1 alors c'est Bob qui va le faire

- Fin du programme et objectif de session SRTP atteint

- Pause repas entre 12h et 13h30

- Étude des secrets pour voir s'il y a bien correspondance

- Départ vers 17h

Mercredi 27 avril :

- Arrivée vers 7h55

- Mise en place de test pour voir si les secrets sont bien partagés

- Tout à l'air d'être ok

- Pause repas entre 12h et 13h30

- Reprise des tests, srtpSecrets notamment, les clefs, les sels etc

- Départ vers 16h15

Jeudi 28 avril :

* Arrivée vers 7h45
* Reprise des tests de comparaisons, tout est ok pour mackey, zrtpkey, KDFContext
* Destruction de s0 dans updateCachedSecrets
* Début de remise en forme du code
* Ajout de fonctions auxiliaires pour simplifier la boucle principale
* Mise au propre de la boucle main
* Pause repas entre 12h et 13h30
* Reprise de la mise au propre du code avec des commentaires
* Départ vers 16h15

Vendredi 29 avril :

* Arrivée vers 8h
* Étude de ce qu’est une signature
* Étude de l’endroit où mettre la signature
* Rédaction d’un plan d’action
* Pause repas entre 12h et 13h30
* Étude du code c de ECDSA
* Réunion avec Loïc entre 14h30 et 15h30
* Départ vers 16h15

Lundi 2 mai :

* Arrivée vers 7h40