Nous voilà alors en 2002. Nous sommes presque arrivés, c’est la dernière étape : on a atteint une méthode qui propose un niveau de sécurité qui n’est pas crackable par des ordinateurs classiques.

Le joueur se trouve dans un petit bureau. En regardant à la fenêtre, il se rend compte qu’il est au MIT. Il cherche, comme à son habitude, dans ses poches ; puis trouve dans sa poche un petit message. Il y lit l’inscription suivante :

« Trouve Ron Rivest. Il est professeur ici et pourra t’aiguiller. Voici le message : »

Et il observe alors un nombre gigantesque, de plusieurs dizaines de chiffres. Le joueur se demande bien comment faire.  
Il retourne le post-it et y voit ceci :

« Tu pourras utiliser cette clé de décryptage : »

Et encore un nombre énorme.

Bien embêté, il continue de chercher dans ses poches et trouve un deuxième post-it, avec une petite feuille vierge et un stylo.

« écris sur ce papier le lieux et la date où tu veux rencontrer M. Rivest, puis pose le dans le coffre-fort au fond de la salle et ferme le coffre. Il t’y retrouvera »

Le joueur écrit donc l’adresse du café qu’il voit à la fenêtre, pour le soir-même. Il pose le message dans le coffre ouvert, puis cherche dans ses poches une clé pour le fermer. Introuvable. Il claque alors la porte puis se rend compte que le coffre s’est fermé tout seul : il n’y avait pas besoin de clé. Alors qu’il sort de la salle, il lit dessus : « Dr. Ron Rivest », et commence à comprendre.

Le soir, le professeur ne manque pas l’heure d’une minute et arrive au café.

« J’ai eu votre message. Et vous savez bien que je suis Ron Rivest, car personne d’autre n’aurait pu ouvrir ce coffre ! »

Le joueur réfléchit une seconde, ce qui semble être trop long pour le professeur.

« Et oui, béta ! Si quelqu’un avait trouvé le coffre avant moi, il n’aurait pas pu l’ouvrir ! Tu as découvert ici le principe de la cryptographie asymétrique. »

Le joueur est encore un peu perplexe, et n’a pas le temps d’en placer une avant que le professeur recommence à parler très vite :

« La méthode qu’on a utilisée t’a permis de t’assurer que seul le détenteur de la clé du coffre pouvait recevoir ton message.  
Tu poses ton message dans un coffre destiné à une personne en particulier, que tu fermes. Tout le monde peut te voir mettre ton papier dans le coffre, même voir vers qui va le coffre. Mais lorsque tu l’as fermé, seul le destinataire peut l’ouvrir. L’expéditeur a donc la certitude de l’identité du destinataire !

On va dire que c’est Alice qui essaie d’envoyer un message à Bob, comme d’habitude. Tout le monde sait où est le coffre de Bob : c’est une clé publique. Alice pose le message dans le coffre et le referme. Ensuite, Bob vient l’ouvrir avec une clé que seul lui possède : c’est sa clé privée.

* Très bien, j’ai compris, dit le joueur en coupant le professeur avant qu’il reparte. Mais comment est-ce que tout cela m’aide à décrypter cet immonde message ? »

Et il montre le message au professeur qui commence à rire.

« Aah, j’ai compris pourquoi on t’a envoyé ici. C’est un chiffrement RSA. Viens dans mon bureau, je ne pourrai pas décrypter ça à la main ! »

Ils retournent dans le bureau du professeur, qui allume son ordinateur, recopie les nombres, tape quelques lignes et dit au joueur : *insérer ici commande pour faire avancer la machine*.  
« Et voilà, le tour est joué !

* ??? Quoi ?
* Le chiffrement RSA a été développé par moi-même et deux de mes collègues (dont les initiales sont S et A…), et nous avons gagné le prix Turing grâce à ça ! On implémente de la cryptographie asymétrique avec des nombres premiers. Le tout est assez compliqué, mais il repose sur le principe suivant, qui est celui qui nous assure la sécurité contre les ordinateurs classiques.  
  On choisit une paire de nombres premiers qu’on multiplie. Il faut que les nombres soient extrêmement grands, on peut aller jusqu’à des centaines de chiffres !  
  Ensuite, en gros, la clé publique est un nombre par lequel on multiplie notre message. Pour retrouver le message original, on multiplie et on divise par d’autres nombres qui sont déterminés à partir de nos deux nombres premiers de base. C’est la clé privée.  
  La faille dans cette méthode, est qu’on peut retrouver la clé privée à partir de la clé publique en factorisant la clé publique, donc en trouvant ses diviseurs premiers. Mais cela est immensément long avec un ordinateur classique, et il faudrait bien des années ! Seul un ordinateur quantique peut le faire rapidement, par exemple avec l’Algorithme de Shor. Mais on ne risque pas de les inventer de sitôt… »

Le joueur rit un peu, puis salue le professeur avant de partir