

Animer une initiation à la cryptographie

(sans être cryptographe)



Résumé Ce document décrit la mise en place d'une activité d'initiation à la sécurité informatique prenant la forme d'une énigme interactive modérée par un animateur.

Animateur : un.e professeur.e de mathématiques, ou du moins une personne de formation scientifique attirée par les casse-têtes. Le document présent forme aux compétences scientifiques techniques requises (aucune familiarité avec la cryptographie supposée).

Public : un groupe de *jusqu'à 20 personnes* environ, enfants ou adultes, *dès 13 ans*.

Durée : idéalement *1h-1h30* (modulable).

Objectifs : faire prendre du recul au public sur la *notion de sécurité* en informatique, et lui faire prendre la mesure de la subtilité de la conception de systèmes sûrs.

Ce document contient environ 10 pages de description (narration et logistique), et environ 5 pages d'exercices annexes corrigés pour s'entraîner aux parties techniques si besoin.

Cette activité a été développée par des chercheurs en informatique dont les contributeurs notables Véronique Cortier, Joseph Lallemand et Itsaka Rakotonirina. Le document présent reprend en particulier plusieurs efforts de diffusion antérieurs [1, 11, 12]. Toutes les images sont sous licence Creative Commons (CC-BY-SA).

Table des matières

1 Un peu de contexte	3
2 L'histoire : l'énigme du livreur glouton	4
2.1 Le décor	4
2.2 Là où tout bascule	5
2.3 Contre un livreur actif	5
2.4 Les livraisons dangereuses	6
2.5 Le comique de répétition	7
2.6 Jusqu'à quand y croirez-vous?	7
3 Avec du public : mise en place	8
3.1 Logistique	8
3.2 Obtention du matériel	9
4 Avec du public : déroulement détaillé et retours d'expérience	10
4.1 Introduction et Problème 1	10
4.2 Attaque et Problème 2	11
4.3 Phase de conception	11
4.4 Phase de compétition	12
4.5 Dernière attaque et conclusion	13
Sources	14
Annexes	15
A Gestion des contraintes horaires	15
B Entraînement technique	15
B.1 Principe fondamental des attaques étudiées	16
B.2 Exercices corrigés	16

1 Un peu de contexte

Les *télécommunications* réfèrent à toute forme de transfert de données à plus moins longue distance. On les trouve tout autour de nous, parfois sans le savoir : un ordinateur communiquant avec une borne wifi ; un paiement en ligne ; une clé de voiture déverrouillant une portière à distance ; et même les puces de nos passeports biométriques interagissant avec les bornes d'aéroport. Tous ces exemples ont deux caractéristiques cruciales en commun :

- 1 les communications en jeu peuvent facilement être *interceptées* : elles circulent autour de nous via des ondes, il suffit donc d'une simple antenne pour les capter ;
- 2 les données communiquées sont *sensibles* : un numéro de carte bancaire, des informations permettant d'usurper une identité, un mot de passe... bref, des messages dont l'interception ou l'alteration peuvent avoir des conséquences sociales, économiques, voire politiques.

Ce cocktail explosif est la motivation derrière la *cryptographie*, la discipline s'attelant à protéger les communications d'interférences extérieures. On trouve des traces de mécanismes cryptographiques dès la Grèce Antique [10] et, plus généralement, la cryptographie a eu une influence géopolitique tout au long de l'Histoire. Un exemple notable est *Enigma*, un système de protection des communications utilisé entre autre par l'Allemagne nazie, et dont le "cassage" par les Alliés est estimé avoir réduit la durée de la Seconde Guerre mondiale d'au moins deux ans, d'après des sources proches des services secrets britanniques de l'époque [3]. Mais aujourd'hui, loin de ces exemples historiques, le monde de la sécurité a de quoi laisser perplexe :

- 1 d'une part, notre principal contact avec la cryptographie est la formule "*100% sécurisé*", omniprésente dans les publicités ou sur internet dès que de l'informatique est en jeu ("paiement 100% sécurisé", "service 100% sécurisé", "messages 100% sécurisés"...);
- 2 d'autre part, la presse fait souvent état de *cyberattaques* spectaculaires (voir, par exemple, les attaques régulières sur des hôpitaux mentionnées dans un rapport de l'Anssi [8]).

Si aujourd'hui tout est 100% sécurisé, pourquoi entend-on autant parler de failles de sécurité ?

Ce document décrit une courte initiation à la sécurité démythifiant cette discipline, en confrontant le public à ses défis technologiques de manière ludique via une énigme interactive. Cette activité ne nécessite aucun matériel informatique, et a été testée de nombreuses fois sur des groupes scolaires à partir de 13 ans (portes ouvertes, cours d'ouverture aux sciences du numérique), des étudiants, et même des adultes curieux (de formation scientifique ou non).

Objectifs de l'activité

- 1 Mise en contact avec les défis de la cryptographie contemporaine et leurs subtilités.
- 2 Comprendre que la sécurité absolue n'a pas de sens, et donner une idée de comment les métiers de la sécurité étudient le problème en conséquence.

Contenu de ce document, pour l'animateur

- 1 Détails du déroulement de l'activité et le matériel nécessaire.
- 2 Formation à des compétences techniques de sécurité informatique nécessaires pour encadrer l'activité (recherche d'attaques simples). Ce document inclut des retours détaillés d'expérience et des exercices, pensés pour former un professeur de mathématiques à encadrer cette initiation aussi bien que le ferait un expert du domaine.

2 L'histoire : l'éénigme du livreur glouton

Tout d'abord, voici le fil narratif de l'activité, sans mention des interactions avec le public dont la logistique et les détails seront donnés par la suite, en Sections 3 et 4.

2.1 Le décor

Bob voudrait acheter un gâteau à la pâtisserie d'Isabelle. La boutique étant trop éloignée pour y aller en personne, il demande une livraison à domicile. Malheureusement, le livreur est connu pour sa gourmandise : il a tendance à manger compulsivement les gâteaux qu'il est censé livrer. De plus, pour des raisons de conjecture économique trop complexes pour de simples mortels, toutes les autres entreprises de livraison ont fait faillite. C'est une situation délicate : Isabelle et Bob ont besoin du livreur, mais savent qu'ils ne peuvent pas lui faire confiance.



En raison de ce problème, ils se procurent chacun un cadenas à clé dans leurs villes respectives ; ainsi, quand ils utiliseront ce service postal peu fiable, ils pourraient mettre les livraisons dans des coffrets cadenacés pour éviter les vols.

Problème 1. En se servant de ces cadenas, comment transféreriez-vous le gâteau depuis la pâtisserie d'Isabelle à la maison de Bob sans risque ?

La difficulté de l'éénigme est que, bien qu'Isabelle et Bob aient tous deux un cadenas, ils ne peuvent pas ouvrir celui de l'autre. Isabelle pourrait mettre le gâteau dans un coffret, le verrouiller, et envoyer la clé à Bob plus tard ; cependant le livreur pourrait alors obtenir à la fois le coffre verrouillé et sa clé, ce qui lui permettrait de l'ouvrir. Il faut donc trouver une solution où Isabelle et Bob gardent toujours leur clé sur eux. Voici une première idée. Dans un premier temps, Isabelle met le gâteau dans un coffre, le verrouille, et le fait livrer à Bob :



Pour l'instant le livreur ne peut pas manger le gâteau, mais Bob ne peut pas non plus ouvrir le coffre. Ce dernier ajoute alors son propre cadenas au coffre de manière à ce qu'il soit verrouillé par les deux, puis retourne le colis à Isabelle :



À la réception du coffret, Isabelle y retire son propre cadenas et le renvoie :

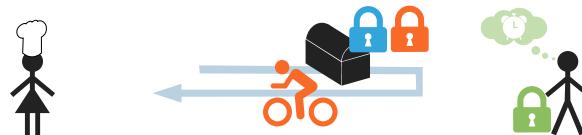


Bob reçoit le gâteau dans un coffre scellé uniquement par son propre cadenas et peut donc le récupérer. Aucune clé n'a été envoyée durant le procédé et il y avait toujours au moins un cadenas sur chaque colis, empêchant le livreur de manger le gâteau. On appelle cela un :

Protocole de sécurité : suite d'instructions permettant d'envoyer un colis sensible à travers un réseau postal corrompu.

2.2 Là où tout bascule

Appelons notre protocole de sécurité par double cadenas V1. Règle-t-il réellement le problème ? Il y a en fait de nombreuses façons pour le livreur de récupérer le gâteau, la plus directe étant de forcer les cadenas avec les outils appropriés. Notre protocole repose donc sur des hypothèses implicites, la première étant que les **cadenas sont incassables**. Une autre est que le livreur n'agit **que sur les livraisons** (il ne cambriole pas Isabelle et Bob pour voler leur clé). Bien que raisonnables, cela fait beaucoup d'hypothèses cachées... Y aurait-il encore autre chose sous le tapis ? Considérons le scénario de livraison suivant. Tout d'abord, Isabelle encoiffe le gâteau avec son cadenas comme d'habitude. Mais là, le livreur **dévie de ses instructions** : au lieu de livrer Bob, il ajoute son propre cadenas — acheté par ailleurs — et retourne le colis.



N'ayant pas conscience qu'il ne s'agit pas du cadenas de Bob, Isabelle pense que le protocole suit son cours sans problème particulier. Elle retire donc son cadenas et demande au livreur de l'apporter à Bob :



La situation finale est alors la suivante : Isabelle n'a rien remarqué de particulier et le livreur peut déverrouiller le coffre avec sa propre clé. Cette *attaque* n'a nécessité de forcer aucun cadenas, elle exploite simplement une brèche dans la structure du protocole. Mais surtout, elle révèle la dernière hypothèse cachée sur laquelle reposait notre solution :

Passivité : malgré sa gourmandise, le livreur ne ment jamais sur le contenu d'un colis, c'est-à-dire, il suit le flot du protocole sans essayer activement de le perturber.

2.3 Contre un livreur actif

Effectuer cette attaque sur V1 ne demande pas un effort énorme au livreur : il n'est donc pas raisonnable de supposer que ce dernier est passif lors de la conception de notre protocole.

Problème 2. Comment envoyer un gâteau depuis la pâtisserie d'Isabelle à Bob sans risque qu'il se fasse manger par un livreur actif ?

Malheureusement, ce problème n'a pas de solution avec notre système de cadenas. Isabelle et ses clients décident donc de souscrire à une organisation à grande échelle de *cadenas publics* :

- 1 tout membre de l'organisation se voit remettre une **clé personnelle**;
- 2 toute personne peut obtenir auprès de l'organisation un cadenas ne pouvant être ouvert que par la clé d'**un membre spécifique**.

On supposera qu'on peut faire entièrement confiance à cette organisation et qu'elle a son propre réseau (non-corrompu) de distribution de cadenas. Un nouveau protocole — appelons-le V2 — garantit alors la résistance au vol contre un livreur actif : Isabelle se procure le cadenas de Bob via l'organisation, l'utilise pour verrouiller le colis du gâteau, et le fait livrer.

2.4 Les livraisons dangereuses

Mais l'histoire ne s'arrête pas là. Vexé de ne pas pouvoir voler le gâteau, le livreur, mauvais perdant, se procure le cadenas de Bob chez l'organisation, et l'utilise pour lui envoyer un gâteau empoisonné avec le message "*Nous vous offrons ce gâteau en remerciement de votre fidélité. La pâtisserie d'Isabelle*". Bob le mange, ce qui révèle une faiblesse du protocole : nous ne pouvons jamais être sûr que l'expéditeur d'une livraison est celui qu'il prétend être. Au retour de Bob de l'hôpital, Isabelle et lui décident de mettre à jour le protocole pour qu'il garantisse une forme d'**authentification**.

Nous vous offrons ce gâteau en remerciement de votre fidélité.

— *La pâtisserie d'Isabelle*



Problème 3. Quel protocole V3 Isabelle et ses clients pourraient suivre sans que 1 le gâteau puisse se faire voler, ni que 2 le client puisse se faire empoisonner ?

La question est complexe : tout ce qu'Isabelle fait, un livreur actif peut le faire, ce qui rend difficile pour elle de produire un colis différenciable à coup sûr d'un colis piégé. Voici une solution possible. Cette fois, le client est celui qui initie le protocole. Pour ce faire il écrit sur un bout de papier un (long) **mot de passe** de son choix qui servira à identifier sa commande. Il l'envoie ensuite à Isabelle dans un coffre scellé avec le cadenas de cette dernière (obtenu auprès de l'organisation), et joint une note au colis indiquant son nom à Isabelle :



À la réception du coffre, Isabelle lit le nom du client sur la note, ouvre le coffre avec sa clé, met le gâteau à l'intérieur à côté du papier où est écrit le mot de passe, puis scelle le tout avec le cadenas du client (obtenu via l'organisation). Elle lui fait ensuite livrer le colis :

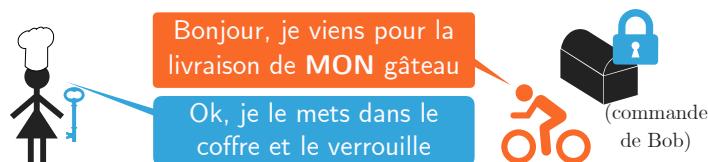


Quand le client reçoit la commande, il vérifie que le gâteau est bien accompagné du même mot de passe qu'il a choisi initialement. Si ce n'est pas le cas il reste prudent, et détruit le

gâteau au cas où il serait empoisonné. Intuitivement, la sécurité de ce protocole V3 repose sur le fait que, pourvu que le mot de passe choisi par Bob soit assez long et imprévisible, si quelqu'un tentait d'envoyer à Bob un gâteau empoisonné en prétendant être Isabelle, il n'aurait qu'une probabilité négligeable de deviner le mot de passe par chance (et donc de faire manger le gâteau piégé à Bob).

2.5 Le comique de répétition

Avec ce protocole, nous avons enfin mis Bob en sécurité, le vol et l'empoisonnement étant à présent impossibles. Vraiment ? Si vous y avez cru, malheureusement, vous vous êtes encore faits avoir : comme pour V1, le raisonnement justifiant la sécurité de V3 était trop informel pour être rigoureux. Ici, V3 ne résout le Problème 3 que sous une hypothèse implicite supplémentaire, qui cachait une autre attaque dans son ombre. Voyez-vous laquelle ? Considérez sinon le scénario de livraison suivant. Le protocole commence comme d'habitude : Bob met un mot de passe dans un coffre verrouillé, et écrit son nom sur une note jointe. Mais en parallèle, le livreur **achète aussi un gâteau** qui sera à récupérer plus tard à la pâtisserie. Il transmet alors la commande de Bob à Isabelle *mais* remplace le nom de Bob par le sien :



Isabelle suit les instructions du protocole et met le gâteau dans le coffre (pensant que le mot de passe qui s'y trouve est celui du livreur), puis le referme *avec le cadenas du livreur*. Ce dernier ouvre alors le coffre, empoisonne le gâteau, et le referme avec le cadenas de Bob.



Le livreur donne ensuite la livraison piégée à Bob, que ce dernier croit sûre à cause de la présence de son mot de passe et mange le gâteau empoisonné. Notre erreur en concevant V3 a été de ne pas protéger l'identité du client, en laissant la note indiquant son nom à l'air libre — ce que peut exploiter le livreur comme dans l'attaque s'il a des **complices parmi les clients** de la pâtisserie ou en est lui-même un. La sécurité de V3 repose donc sur le fait que le livreur n'achètera jamais de gâteau — une hypothèse une fois de plus trop forte pour être raisonnable. Une contre-mesure naturelle est que le client mette la note avec son nom *à l'intérieur* du coffre, à côté du mot de passe, pour empêcher le livreur d'y toucher. Si on appelle V4 cette version corrigée du protocole, elle permet donc d'éviter ce genre d'attaques.

2.6 Jusqu'à quand y croirez-vous ?

Après V1 et V3, cela fait quand même deux fois que vous vous faites servir un protocole qui semblait offrir les garanties de sécurité attendues, avant de vous rendre qu'il y avait en fait une attaque en embuscade. Alors comment y croire cette troisième fois ? La réponse est simple : *rien* ne permet raisonnablement d'y croire, du moins pas seulement sur la base d'arguments

informels comme ceux qui vous ont été fournis. C'est la morale de toute cette histoire : la sécurité est une affaire extrêmement subtile et contre-intuitive, jamais aussi simple et binaire qu'elle peut en avoir l'air au premier abord. Vous l'avez vu tout du long : la plupart des attaques étaient dûes à des argumentations qui, bien que convaincantes, étaient trop peu rigoureuses et reposaient sur des hypothèses implicites déraisonnables. Tout cela est en fait une métaphore de la ***cybersécurité*** :

- 1 le gâteau représente une *donnée sensible*, i.e., dont il est crucial qu'elle reste secrète (confidentialité) et ne se fasse pas altérer (intégrité). Exemple classique : les données bancaires ;
- 2 les cadenas représentent la *cryptographie*, plus précisément différents types de chiffrement, rendant un message inintelligible pour qui ne possède pas une clé de déchiffrement ;
- 3 le livreur représente un *réseau de communication sensible aux interceptions* (comme Internet, où il est possible d'interférer avec un signal en prenant le contrôle d'un relais).

Vous comprendrez donc pourquoi, quand il est question de cybersécurité, il est apprécié que les garanties prétendues d'un système soient soutenues par une **démonstration** rigoureuse. En bref, une définition mathématique du protocole étudié et de la garantie de sécurité attendue, ainsi qu'une démonstration qu'elle est bien effective.

À emporter chez vous Mais tous ces messages sont bien techniques, et il est peu probable que vous en ailliez la moindre utilité dans votre vie quotidienne. Retenez simplement que :

- 1 *La sécurité est une affaire complexe, mais surtout subtile.* Rien n'est "100% sécurisé", "inviolable", toute sécurité n'est valable que sous certaines hypothèses, souvent techniques à comprendre pour le profane. *Au quotidien, gardez donc du recul vis-à-vis des publicités ou gros titres de journaux avec des formules un peu trop optimistes !*
- 2 *La sécurité est un problème étudié par les scientifiques.* Des générations chercheurs se sont succédés pendant des décennies pour étudier beaucoup des systèmes déployés autour de nous, et ont conscience depuis bien longtemps des problèmes auxquels vous avez été confrontés dans ce document. *Au quotidien, gardez donc du recul vis-à-vis des publicités ou gros titres de journaux avec des formules un peu trop pessimistes !*

3 Avec du public : mise en place

3.1 Logistique

D'expérience, les publics d'entre **10 et 20 personnes** ont un bon équilibre : il y a assez de monde pour ne pas intimider les participants avec les énigmes, et assez peu pour que tous puissent participer. De plus, la dernière partie de l'activité nécessite de séparer le groupe en **2 à 4 équipes de 3 à 5 personnes** pour une compétition, ce qui convient justement à des effectifs d'une quinzaine de personne. Cette compétition a également été testée avec succès avec une équipe unique (le public contre l'animateur) pour des publics très réduits ; cela réduit néanmoins significativement son côté ludique, et le public s'est montré moins réceptif aux messages de conclusion de l'activité. Au delà de 4 équipes, la compétition peut devenir compliquée à gérer. Le tout a été testée avec tous publics **à partir de 13 ans** (scolaires, étudiants, adultes curieux). Dans le cadre d'une journée de cours, des enfants de moins de 12 ans auraient probablement des problèmes d'endurance, les énigmes demandant beaucoup de concentration. Les adultes sont en revanche un bon public en général indépendamment de leur

âge, comprenant que la présentation d'apparence enfantine abstrait un problème plus sérieux. Un temps total idéal est de **1h30**, mise en place et conclusion incluses (voir détails en Section 4, et discussions en Annexe A quant aux contraintes horaires du milieu scolaire). Enfin le matériel, listé ci-dessous, rend les énigmes plus visuelles afin de stimuler la compréhension et l'inventivité du public (beaucoup manquent d'idées jusqu'à avoir les jouets entre les mains). Il doit donc être fourni **pour chacune des équipes** de la compétition finale :

- 1 **2 gâteaux** (jouets, jetons, images...);
- 2 **3 cadenas à clé** identifiables (par des couleurs différentes, des étiquettes...). *Conservez un double des clés, au cas où une se fait verrouiller à l'intérieur d'une boîte par le cadenas qu'elle ouvre ;*
- 3 **1 boîte** (idéalement **2 ou 3**) verrouillable par cadenas assez grande pour y mettre un gâteau. *Les boîtes doivent pouvoir être fermées par 2 cadenas à la fois.*
- 4 des **post-it** et **stylos** pour envoyer des messages ;
- 5 **4 figurines** (3 peuvent suffire) pour les personnages.

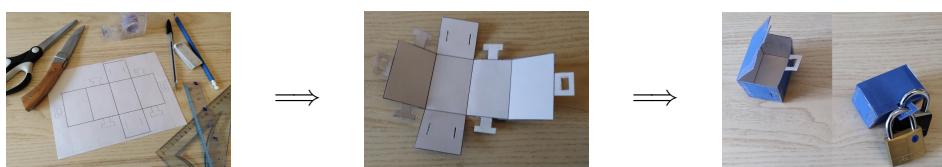


3.2 Obtention du matériel

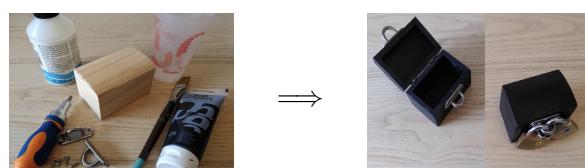
Pour les gâteaux et figurines, prenez des jouets traînant chez vous ou votre famille proche, ou simplement des pièces d'échec, ou pièces de bois à peindre en magasin de **loisir créatifs**. Les cadenas, eux, se trouvent souvent en **magasin de bricolage** (attention aux anneaux trop petits). Des coffres existent aussi dans le commerce, permettant néanmoins rarement d'y placer deux cadenas à la fois. Quelques alternatives :



— **Coffres en carton** La solution la plus simple et économique, bien que pas la plus durable. Tracez simplement le **patron d'un pavé aux dimension de votre choix** sur un papier cartonné de bonne qualité, et découpez puis montez-le. N'oubliez pas d'inclure dans votre patron **deux languettes** qui serviront de support pour attacher vos cadenas !



— **Coffres en bois** Une solution demandant un peu plus d'investissement en temps, mais avec un meilleur rendu visuel et à l'épreuve du temps et du transport. Procurez-vous des coffrets en bois dans un magasin de **loisirs créatifs**, deux **anneaux vissables en métal** trouvables dans un magasin de bricolage sous le nom de *platinas à œil*, et vissez-les de part et d'autre de l'ouverture du coffre. Les anneaux serviront alors de support aux cadenas (attention aux dimensions!). Pour un meilleur rendu, n'hésitez pas à peindre les coffres au préalable avec de la **peinture acrylique** (1 ou 2 couches), à recouvrir de **vernis colle** ou à bois après séchage.



— **Poupées russes** Il peut être intéressant d'avoir plusieurs tailles de boîtes permettant de les emboîter comme des poupées russes (cadenas inclus). Bien que ce mécanisme ne soit pas nécessaire à l'activité, sa mise à disposition a souvent un effet formateur. En effet, le public part souvent du principe que “*si c'est là, c'est que c'est utile*”, ce qui est une mauvaise pratique en sécurité : ajouter toutes les dernières technologies à disposition ou à la mode ne rend pas un système plus sûr ou plus performant !

⚠ **Conditions sanitaires** L'activité reposant sur la manipulation de matériel par des groupes, il convient de garder des réserves sur son déploiement dans un éventuel contexte épidémique tendu. Si les réglementations en vigueur autorisent la tenue de l'activité, des précautions restent malgré tout les bienvenues (nettoyage du matériel au spray désinfectant en amont, utilisation de gel hydroalcoolique pour le public avant les manipulations).

4 Avec du public : déroulement détaillé et retours d'expérience

Cette section décrit comment organiser une séance d'initiation à la cryptographie basée sur l'histoire présentée en Section 2, et en utilisant le matériel en Section 3. Sont inclus des retours d'expérience, ainsi que des anecdotes historiques et techniques pouvant ponctuer l'animation.

4.1 Introduction et Problème 1

⌚ 15 min

Après quelques minutes d'installation, l'activité commence avec une brève mise en contexte pouvant reprendre la Section 1, en expliquant que le but de la séance est de se plonger dans le sujet en mettant la main à la pâte, via une énigme où la cryptographie est représentée par des coffres et cadenas. On passe ensuite à la présentation de l'énigme elle-même, en utilisant le matériel en illustration, jusqu'à poser le Problème 1 au public (voir Section 2.1).

Retours d'expérience

— **Interaction avec le public** Il est important que cette première phase de l'activité soit interactive et mette le public à l'aise avec le format ludique. Les plus jeunes n'hésitent en général pas à proposer des idées, même simples et qui ne fonctionnent souvent pas — mais cela permet de faire avancer la réflexion du groupe. Au contraire, les participants plus âgés identifient souvent mieux les défauts de leurs solutions et appréhendent donc souvent plus de prendre la parole. Il ne faut donc pas hésiter à inciter à proposer des idées, même s'ils savent qu'elles ne marchent pas, en leur expliquant que les formuler à haute voix aide à identifier les difficultés à résoudre. Une autre possibilité est de lancer le mouvement en proposant soi-même des solutions erronées, et de demander au public d'identifier pourquoi elles ne fonctionnent pas. En cas de question sur ce que peut faire chaque personnage :

- 1 Le livreur peut faire n'importe quoi avec ce qu'on lui donne (i.e., pas de cambriolage pour voler le gâteau ou les clés), et ne peut pas ouvrir un cadenas sans sa clé.
- 2 Isabelle et Bob peuvent faire n'importe quoi tant que tout passe par le livreur (pas de communication par un canal annexe comme le téléphone par exemple). On considère aussi qu'il faut la clé pour fermer un cadenas.

— **Propositions fréquentes** La plupart des protocoles sont *attaquables* (i.e., le livreur peut voler le gâteau) ou *invalides* (i.e., ne respectent pas l'énoncé). Quelques exemples :

- 1 **Attaquable** : *Isabelle envoie un coffre verrouillé avec le gâteau, puis la clé ultérieurement.* Le livreur peut alors obtenir le coffre verrouillé et la clé du cadenas.
- 2 **Invalidé** : *Isabelle envoie un coffre verrouillé, attend un appel téléphonique de Bob comme accusé de réception pour s'assurer que le livreur n'a plus le colis, puis envoie la clé.* Les canaux de communication annexes comme le téléphone sont interdits. La difficulté est précisément de lutter contre un attaquant contrôlant toutes les communications.
- 3 **Attaquable** : *Même chose, mais l'accusé de réception est un colis quelconque envoyé par Bob.* Le livreur peut très facilement fabriquer un faux accusé de réception. De toute façon, dans la vraie vie où les coffres verrouillés sont des messages chiffrés, le livreur pourrait facilement garder une *copie* du colis : ces solutions à base d'accusés de réception n'ont donc pas d'intérêt en dehors de l'activité, et nous les mettons donc de côté.
- 4 **Invalidé** : *Bob envoie son cadenas ouvert à Isabelle, qui l'utilise pour fermer le colis du gâteau, et l'envoie à Bob.* Isabelle a besoin de la clé de Bob pour fermer le cadenas.

4.2 Attaque et Problème 2

⌚ 10 min

Une fois la solution (V1) trouvée, l'animateur fait venir deux volontaires pour jouer le protocole physiquement, avec les coffres et les figurines : un jouera d'Isabelle, l'autre Bob, et l'animateur le livreur. Ne pas hésiter à le faire plusieurs fois. Une fois le public à l'aise avec le protocole, l'animateur le fait jouer une fois de plus mais réalise cette fois l'attaque sur V1 (voir Section 2.2). C'est le moment de parler des livreurs passifs et actifs, d'introduire l'organisation gérant les cadenas publics, et de laisser le public résoudre rapidement, oralement, le Problème 2 (voir Section 2.3).

► Détails et anecdotes : Le système initial de cadenas (où ils sont ouverts et fermés par la même clé) représente ce qu'on appelle le **chiffrement symétrique**. En revanche, le système de cadenas publics s'appelle le **chiffrement asymétrique** : tout le monde peut obtenir et fermer le cadenas de tout le monde, mais chacun ne peut ouvrir que le sien. Le chiffrement asymétrique, bien que plus puissant, nécessite cependant de mettre en place cette fameuse organisation fournissant les cadenas. Ici, nous lui faisons aveuglément confiance ; mais dans la vraie vie, c'est un problème complexe nécessitant de déployer des mécanismes de **certificats**. Si Isabelle demandait un cadenas mais qu'on lui en fournissait un autre, le gâteau serait à nouveau menacé ! Vous avez d'ailleurs probablement déjà été confrontés au problème sur le web. Parfois, le navigateur rechigne à entrer sur un site car “*le certificat n'est pas valide*” : cela signifie soit que 1 quelqu'un essaie d'usurper “l'identité” du site avec un faux certificat pour vous piéger, soit 2 le site n'a pas ses certificats à jour.

4.3 Phase de conception

⌚ 25 min

On passe alors à la partie principale, où le public conçoit son propre protocole. On commence par montrer l'attaque par empoisonnement sur V2 avec les jouets. On pose ensuite le

Problème 3 (voir Section 2.4), puis sépare le public en **2 à 4 équipes de 3 à 5 personnes**, qui vont réfléchir au problème chacune de leur côté. Chacune reçoit aussi un minimum de **matériel** pour jouer physiquement les protocoles (boîte, figurines pour les personnages dont éventuellement l'organisation, 3 cadenas, post-it et stylo pour glisser des messages dans les colis). Après un temps de recherche en autonomie, pensez à **circuler dans les groupes** pour encourager ceux ayant du mal à démarrer, et signaler les protocoles invalides... mais **pas les attaques!**

Retours d'expérience Voici des exemples de protocoles *invalides* vus sur le terrain :

- 1 **Utilisation de canaux de communication annexes**. Comme précédemment, les communications ne passant pas par le livreur (téléphone par exemple) sont interdites.
- 2 **Sécurité par obscurité** : “*Isabelle envoie cette boîte en prétendant qu'elle contient un message, alors qu'en fait c'est un gâteau, mais le livreur n'a aucun moyen de le savoir.*” On voit souvent ce genre de propositions reposant sur le fait que le livreur ne connaît pas le protocole utilisé. Mais **le protocole ne peut pas être secret** : Isabelle l'utilise avec tous ses clients, dont le livreur (qui a aussi le droit d'acheter des gâteaux) !
► **Détails et anecdotes** : La sécurité par obscurité était déjà considérée comme une mauvaise pratique dans les principes de Kerckhoffs [5] en 1883, dans le contexte militaire. Aujourd'hui cela n'a pas changé : si la sécurité d'une entreprise repose sur le secret de son système, un employé part chez le concurrent et tout s'écroule !
- 3 **Signature**. Il peut arriver que, pour authentifier un colis, des groupes fassent *signer* un papier par Isabelle. Les **signatures digitales** existent en cryptographie mais ont des propriétés cruciales, en particulier que ***a*** il est très difficile (impossible) d'imiter une signature valide de quelqu'un, et ***b*** une signature valide sur un document subissant ultérieurement une modification perd sa validité. Dit autrement, trouver une signature valide sur un gâteau doit garantir que personne ne l'a empoisonné depuis sa signature. Une signature papier n'a en général aucune de ces propriétés, et on les évite donc ici.
- 4 **Déni de service** : “*Livreur peut juste voler le coffre verrouillé : ok, il ne pourra pas manger le gâteau, mais Bob ne recevra jamais son colis. C'est un problème, non ?*” En bref : non, du moins pas ici. Bien sûr, cela embêterait Bob, mais garantir qu'une livraison arrive à destination n'est pas un problème qui se règle avec des cadenas. La sécurité soulève des centaines de questions, chacune s'étudiant avec des outils différents : et le problème étudié dans cette activité est de savoir si on peut, avec des cadenas, empêcher le livreur de **manger** le gâteau ou de l'**empoisonner**. Garantir que la livraison arrive à bon port se fait par d'autres moyens, qu'on va donc ignorer aujourd'hui.
► **Détails et anecdotes** : bloquer systématiquement une communication est appelé un ***déni de service*** (ou *DoS* pour *denial of service*). Ce genre d'attaques (illégales) est fréquemment utilisé par des entreprises pour perturber les concurrents, majoritairement dans le milieu des Télémcs et de la finance [6]. Le problème est également très présent dans... le jeu vidéo, où des équipes d'e-sport s'attaquent parfois pendant en compétition.

4.4 Phase de compétition

 15 min

Une fois la réflexion en équipe terminée, deux volontaires par groupe passent pour jouer leur proposition de protocole devant les autres. Ils jouent respectivement Isabelle et Bob,

et l'animateur joue le livreur ***de manière honnête***, c'est-à-dire, il n'essaie pas de voler le gâteau ou d'empoisonner Bob. Les autres groupes cherchent ensuite une attaque, c'est-à-dire, expliquent à l'animateur ce qu'il devrait faire pour empoisonner Bob.

⚠ Compétence technique Si le public ne trouve pas d'attaques sur la solution d'un groupe, l'animateur doit savoir déterminer ***s'il n'en existe effectivement pas*** (en omettant les attaques du même type que sur V3, où le livreur doit lui-même être client de la boulangerie). Cela demande un peu d'entraînement : de la méthodologie et des exercices corrigés sont compilés en ***Annexe B*** si besoin.

Retours d'expérience Les groupes présentent leur protocole *en l'état*, même s'ils n'en sont pas satisfaits : cela fait toujours un entraînement pour les autres groupes !

► **Anecdote** : La technique utilisée dans la solution, le protocole V3, est connue sous le nom de *challenge-response* et est largement utilisée, par exemple dans les protocoles de paiement [2] et les passeports biométriques [4]. Ici par exemple, Bob émet le “challenge” de lui renvoyer un gâteau accompagné de son long mot de passe temporaire : Isabelle étant la seule à pouvant ouvrir cette boîte, elle est ainsi censée être la seule à pouvoir répondre au challenge (même si, ici, une faille de structure permet au livreur d'y répondre également comme le montre l'attaque sur V3 détaillée en Section 2.5).

4.5 Dernière attaque et conclusion

 10 min

À ce stade, le public est en général assez fatigué mentalement, et a bien compris que le problème n'était si simple. En fonction du temps et de la réactivité des groupes, il y a alors le choix entre : 1 directement conclure (en reprenant des éléments de la Section 2.6), éventuellement en mentionnant qu'il existe une attaque, que le public pourra chercher chez lui si cela l'intéresse, si le livreur est client de la pâtisserie ; 2 ou alors, avant cela, de présenter la dernière attaque sur V3 (voir Section 2.5), et la correction pour obtenir V4.

Retours d'expérience Il peut arriver que certaines équipes aient trouvé un protocole résistant à cette attaque (en bref, un équivalent V4 où Bob écrit son nom à l'intérieur de sa commande). Dans ce cas, il est possible de présenter V3 comme le protocole d'une équipe fictive, disons la votre, et de donc demander au public ce qu'ils pensent du protocole.

► **Anecdote** : Ce protocole de livraison de gâteaux (V3) est inspiré d'un protocole réel, dit de *Needham-Schroeder* du nom de leurs inventeurs [9]. Comme ici, il souffre d'une attaque similaire à celle de V3. Cette attaque a seulement été découverte une vingtaine d'années après la publication du protocole, par Lowe [7], montrant que la recherche d'attaques n'est pas simple, même pour les experts y consacrant tout leur temps. Le problème étant que les analyses de l'époque avaient tendance à omettre inconsciemment la possibilité que l'*attaquant* (le livreur dans lénigme) ait la possibilité d'interagir avec les participants en tant que simple personne (acheter un gâteau dans lénigme).

Sources

- [1] Véronique CORTIER et Itsaka RAKOTONIRINA : How to explain security protocols to your children (en anglais). In *Protocols, Logic, and Strands : Essays Dedicated to Joshua Guttman on the Occasion of His 66.66 Birthday (GuttmanFest2021)*, 2021.
- [2] EMVCo : Book1 – application independent ICC to terminal interface requirements (en anglais). Rapport technique, November 2011.
- [3] Harry HINSLEY : The influence of ultra in the second world war (en anglais), 19 octobre 1993. Transcript d'une conférence donnée par Harry Hinsley, historien ayant côtoyé l'équipe de cryptanalyse d'Enigma durant la seconde guerre mondiale. Consultable en ligne à https://www.cdpa.co.uk/UoP/HoC/Lectures/HoC_08e.PDF (lien accédé le 13 septembre 2021).
- [4] ICAO : Machine readable travel documents (en anglais). Rapport technique, International Civil Aviation Organization, 2006. Doc 9303. Part 1.
- [5] Auguste KERCKHOFFS : La cryptographie militaire. In p. 5–38 vol. IX, éditeur : *Journal des sciences militaires*, Janvier 1883. disponible en ligne à https://www.petitcolas.net/kerckhoffs/crypto_militaire_1.pdf (lien accédé le 18 septembre 2021).
- [6] Kaspersky LAB : Denial of service : How businesses evaluate the threat of DDoS attacks (en anglais). Rapport “IT Security Risks Special Report Series”, disponible en ligne à https://media.kasperskycontenthub.com/wp-content/uploads/sites/45/2018/03/08234158/IT_Risks_Survey_Report_Threat_of_DDoS_Attacks.pdf (lien accédé le 17 septembre 2021), 2015.
- [7] Gavin LOWE : Breaking and fixing the Needham-Schroeder public-key protocol using FDR (en anglais). In *Tools and Algorithms for the Construction and Analysis of Systems (TACAS'96)*, 1996.
- [8] Agence nationale de la sécurité des systèmes d'information (ANSSI) : État de la menace rançongiciel à l'encontre des entreprises et institutions, 5 février 2020. Consultable en ligne à <https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-001.pdf> (lien accédé le 13 septembre 2021).
- [9] Roger NEEDHAM et Michael SCHROEDER : Using encryption for authentication in large networks of computers (en anglais). *Communication of the ACM*, 1978.
- [10] PLUTARQUE : *Vies parallèles*. Paris, Gallimard, coll. “Quarto”, 2001. Traduit du grec ancien par A.-M. Ozanam, extrait “Vie de Lysandre, §XIX” mentionnant le Scytale, mécanisme utilisé par les Spartiates au V^e siècle av. J.C. pour coder des messages militaires.
- [11] Itsaka RAKOTONIRINA : *Efficient verification of observational equivalences of cryptographic processes : theory and practice*. Thèse de doctorat, Université de Lorraine, 2021.
- [12] Itsaka RAKOTONIRINA : Les livraisons dangereuses, January 2021. Sur le site Interstices : <https://interstices.info/les-livraisons-dangereuses/>.

Annexes

A Gestion des contraintes horaires

De bout en bout, l'activité dure environ **1h15**, ce qui est souvent adapté aux cadres dédiés (ateliers lors de visites de laboratoire, fêtes de la science ou analogues...). Cela peut être plus compliqué en milieu scolaire où les cours sont souvent par créneaux de 55min. Possibilités :

- 1 **Trouver un créneau de 2x55min consécutives de cours.** Le cadre le plus adapté pour les classes de collège, une classe entière pouvant faire office de groupe (plus complexe pour le lycée où il faudrait plutôt une demi classe). Dans ce cas, une pause d'une dizaine de minutes peut être laissée aux élèves entre les deux créneaux, ce qui tombe souvent vers la fin de la phase de conception. En prenant son temps, l'activité s'étend ainsi facilement sur 1h40 environ. On peut alors compléter avec une séance de questions ou d'anecdotes sur le sujet ; les classes de collège apprécieront par exemple qu'on parle d'exemples concrets comme le *code de César*... et surtout sur comment le casser par *analyse fréquentielle*, toutes les notions de mathématiques nécessaires étant justement au programme de collège !
- 2 **Faire la séance sur deux créneaux non consécutifs de 55min.** L'analogue de la solution précédente pour les classes de lycée, ayant rarement plusieurs créneaux consécutifs en demi groupe. On fait la césure après la phase de conception, laissant la fin de l'activité à la séance suivante (en demi groupe ou classe entière). Bien que cela casse un peu le rythme de l'activité, la seconde séance garde un côté dynamique avec la compétition de la phase de restitution. Une fois la conclusion passée, il peut rester du temps pour poursuivre sur un cours classique, idéalement un sujet connexe pour les cours de sciences et technologie.
- 3 **Faire la séance sur 55min.** Cela est possible, mais nécessite de faire quelques coupes. En comptant 5min d'installation et de 5min rangement, il reste environ 45min d'activité pure. Un bon découpage est alors de 5min de d'introduction, 10min pour l'énigme initiale, 15min pour la phase de conception, 10min pour la phase de restitution, et 5min de conclusion. On se limite alors à mentionner qu'une attaque sur V3 existe si le livreur est client de la pâtisserie, sans la présenter, laissant les intéresser la chercher chez eux. Il ne faut pas traîner et éviter les détails et anecdotes, mais cela reste faisable en petit comité.

B Entraînement technique

Dans cette section finale sont compilés quelques conseils et exercices pour entraîner un non-expert en cryptographie à encadrer la phase de compétition (voir Section 4.4). Aucune familiarité n'est pré-requise avec le domaine, mais la nature mathématique du problème pourrait rebuter les éventuels allergiques à la matière.

B.1 Principe fondamental des attaques étudiées

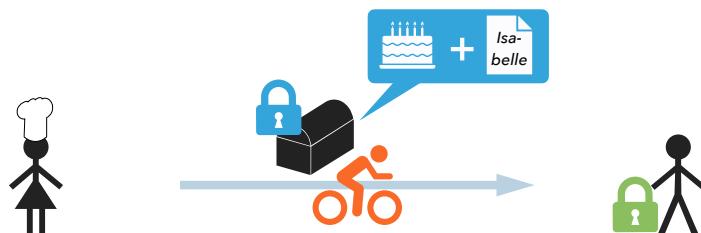
La plupart des attaques de l'activité reposent sur une observation simple :

Principe fondamental *En dehors de l'utilisation de leur clé, toute action effectuable par Isabelle ou Bob peut également être effectuée par un livreur actif.*

Par exemple, l'attaque sur V1 (Section 2.2) utilise le fait que le livreur “imité” Bob : Bob doit ajouter son cadenas sur le colis qu'Isabelle lui envoie et le renvoyer, et c'est exactement ce que le livreur fait. L'attaque sur V2 (Section 2.4) suit la même logique : Isabelle envoie ses gâteaux simplement sans aucune preuve de provenance, et le livreur peut donc faire de même avec un gâteau empoisonné. Le protocole V3 est le premier de la série avec une forme d'authentification, via le mot de passe temporaire de Bob, d'où le fait que son attaque (Section 2.5) soit un peu plus subtile. Mais le but de la phase de conception étant précisément d'arriver à une sécurité du niveau de V3, vous ne serez confrontés qu'à des propositions soit “aussi sûres que V3”, soit attaquables en utilisant principalement le principe fondamental.

- Remarque : Le nom de “*principe fondamental*” n'est pas classique — ce n'est d'ailleurs pas du tout un principe central de la théorie de la sécurité. Il fallait cependant bien lui donner un nom dans ce document, au vu du nombre de fois dont nous allons en avoir besoin.

Voici un exemple simple, pour illustrer ce fameux principe en plus des attaques sur V1 et V2. Puisque le problème de V2 est que Bob ne peut pas savoir si un colis d'Isabelle ou pas, ils mettent à jour le protocole simplement en demandant à Isabelle d'ajouter son nom à l'intérieur du colis en plus du gâteau :



Naturellement, cette solution est très naïve, et il suffit d'appliquer le principe fondamental à Isabelle pour le voir : si Isabelle peut écrire son nom à l'intérieur d'un coffre, le livreur peut tout aussi bien écrire “*Isabelle*” à côté de son gâteau empoisonné, résultant en une attaque.

B.2 Exercices corrigés

Pour conclure ce document, voici une série d'exercices compilant des situations concrètes (la plupart ayant été rencontrées sur le terrain). Chaque exercice décrit les étapes d'un protocole, supposément proposé par une équipe lors de la phase de conception, sa description étant ponctuée d'arguments (valides ou pas) comme vous pourriez typiquement entendre en pratique. L'objectif à chaque fois est de :

- 1 *Déterminer si le protocole est valide ou pas*, i.e., si le protocole utilise des mécanismes interdits (le cas échéant, il faut le signaler à l'équipe en question lors d'une activité).
- 2 *Déterminer si le protocole est attaquable*, en supposant que le livreur n'est pas client de la boulangerie. Pour rappel, cela est à garder pour vous lors de la phase de conception.

Exercice 1 :

- 1 Isabelle initie le protocole en choisissant un long mot de passe, qu'elle écrit sur un papier, qu'elle met dans un coffre fermé avec le cadenas de Bob et fait livrer le tout.
- 2 Bob retire le cadenas, lit le mot de passe et renvoie le colis à Isabelle après l'avoir fermé avec le cadenas de cette dernière.
- 3 À la réception, Isabelle vérifie que le coffre contient bien le même mot de passe que celui qu'elle a mis initialement. Si c'est bien le cas, elle a l'assurance qu'elle communique bien avec Bob, et peut donc lui envoyer le gâteau seul dans un coffre fermé avec le cadenas de Bob.

Solution.

Le protocole est valide (toutes les opérations qu'il réalise sont autorisées). En ce qui concerne la sécurité, bien que le début du protocole puisse paraître intéressant avec une utilisation de mot de passe, tout s'écroule à l'étape 3 où Isabelle envoie finalement le gâteau sans aucun mot de passe, ce qui rend le colis final complètement décorrélé des étapes précédentes. Un attaque simple est par exemple pour le livreur de laisser les deux premières étapes se passer normalement, puis de mettre un gâteau empoisonné dans un colis fermé avec le cadenas de Bob, et de livrer le tout à ce dernier en prétendant qu'il s'agit du colis final d'Isabelle. □

Exercice 2 :

Même protocole qu'à l'Exercice 1, sauf qu'à l'étape 3, Isabelle met le mot de passe *avec* le gâteau. À la réception de ce colis, Bob ne mange le gâteau que s'il est accompagné du mot de passe qu'il a lu à l'étape 2 du protocole.

Solution.

Le protocole est tout aussi valide qu'à l'Exercice 1, et a cette fois une dernière étape utilisant l'échange de mot de passe effectué préalablement. La solution ressemble d'ailleurs à V3 — qui est pour rappel considérée comme sûr pendant l'activité puisque le livreur ne peut pas l'attaquer sans acheter lui-même de gâteau. La seule différence est qu'ici, *Isabelle* choisit le mot de passe ; et c'est ce qui rend le protocole attaquable, en utilisant le principe fondamental. En effet, le livreur peut simplement imiter Isabelle, c'est-à-dire, initier des échanges avec Bob en lui envoyant tout ce que Isabelle lui aurait envoyé :

- 1 Le livreur choisit un mot de passe et l'envoie à Bob dans un coffre fermé.
- 2 Ce dernier lui renvoie le colis fermé avec le cadenas d'Isabelle. Le livreur ne peut pas l'ouvrir mais peu importe car il connaît son contenu (le mot de passe qu'il a lui-même choisi). Il jette donc le colis à la poubelle, et en fait un autre contenant le mot de passe écrit sur un nouveau papier et un gâteau empoisonné.
- 3 Bob trouve bien le mot de passe qu'il a lu précédemment, et se fait donc empoisonner.

Morale : le but étant de protéger *Bob*, puisque le livreur peut toujours imiter Isabelle, Bob doit participer activement au processus d'authentification (comme dans V3) sous peine d'être sujet à une attaque du même type que ci-dessus. □

Exercice 3 :

- 1 Isabelle fait un double de sa clé et l'envoie à Bob dans un coffre fermé avec le cadenas de ce dernier.
- 2 Une fois la clé reçue, on se retrouve dans la situation du tout début de l'activité, sauf que Isabelle et Bob partagent la clé d'un même cadenas. Isabelle peut donc envoyer le gâteau dans un coffre fermé par son propre cadenas sans risque d'interception.

Solution.

Le protocole est valide, mais l'argumentation comparant le protocole avec le début de l'activité est une immense arnaque : non, on ne se retrouve pas du tout dans la même situation qu'au début de l'énigme, puisque n'importe qui peut contacter l'organisation pour obtenir les cadenas de n'importe qui. L'attaque consiste donc simplement à laisser Isabelle donner sa clé à Bob, puis à envoyer à Bob un gâteau empoisonné dans un coffre fermé avec le cadenas d'Isabelle. □

Exercice 4 :

- 1 Isabelle envoie tout d'abord un colis vide à un client tiers (appelons-le Charlie).
- 2 Pendant que le livreur est occupé à faire cette livraison, Isabelle et Bob se rencontrent pour faire l'échange de gâteaux en main propre sans risque d'interférence.

Solution.

Cette solution est *invalidée*, et de manière générale, envoyer des boîtes vides est inutile (tous les colis doivent de toute façon passer par le livreur : l'occuper ailleurs ne fait que retarder la prochaine étape du protocole, sans avantage en contrepartie). Si Isabelle et Bob pouvaient se rencontrer en personne pour s'échanger le gâteau, ils auraient pas besoin du livreur en premier lieu ; et surtout, il n'y aurait aucune nécessité de l'occuper ailleurs non plus. □

Exercice 5 :

- 1 Isabelle envoie un gâteau *empoisonné* à Bob, dans un coffre sans cadenas.
- 2 Si ce dernier ne le reçoit pas, c'est que le livreur l'a mangé et est donc mort, et Isabelle et Bob peuvent alors se retrouver sans risque d'interférence.
- 3 Si Bob reçoit le gâteau, c'est que le livreur n'a pas l'intention d'interférer avec le protocole, et Isabelle peut envoyer un gâteau (non empoisonné) sans danger, dans un coffre fermé avec le cadenas de Bob.

Solution.

Cette solution est *invalidée*. Tout d'abord, il est absurde de “tuer” le livreur, puisque toutes les communications doivent passer par lui. Par ailleurs, si Isabelle et Bob pouvaient se retrouver en personne pour s'échanger le gâteau, le protocole serait inutile de toute façon. Enfin, le dernier point fait des hypothèses fortes sur le raisonnement du livreur, ce qui est déraisonnable puisqu'il sait ce qu'Isabelle et Bob prévoient de faire (voir protocoles par obscurité, point 2 p.12). □

Exercice 6 :

- 1 Isabelle choisit tout d'abord un long de passe m et met le gâteau et m (écrit sur un papier) dans un coffre fermé avec son *propre* cadenas. Appelons le colis verrouillé qui en résulte c_1 .
- 2 Isabelle met ensuite le colis c_1 dans une boîte plus grande, y ajoute un autre papier avec m écrit dessus, puis ferme le tout avec le cadenas de Bob. Appelons ce nouveau colis c_2 , qui est envoyé à Bob.
- 3 À la réception de c_2 , Bob retire son cadenas, lit le mot de passe m à l'intérieur, puis referme la boîte avec le cadenas d'Isabelle. Appelons ce nouveau colis c'_2 , qui est envoyé à Isabelle.
- 4 À la réception de c'_2 , Isabelle retire son cadenas pour obtenir c_1 qui se trouve à l'intérieur (et qui, pour rappel, contient le gâteau et un papier avec m). Elle enlève le cadenas de c_1 et le remplace par le cadenas de Bob, et lui envoie le colis c'_1 résultant.
- 5 À la réception de c'_1 , Bob retire son cadenas, et vérifie qu'il contient un gâteau et le mot de passe m qu'il a lu à l'étape 3. Si c'est le cas, il peut manger le gâteau.

Solution.

Ce protocole est assez long à décrire, mais offre ainsi un bon entraînement à gérer les propositions denses (ce qui peut arriver en pratique, bien que rare), et avec des boîtes en poupées russes. Ce protocole est valide mais, malgré sa complexité, peut se casser très simplement en utilisant encore le principe fondamental. Le problème est similaire à l'Exercice 2 : rien n'empêche le livreur de simplement imiter Isabelle auprès de Bob car ce dernier n'est pas activement engagé dans le choix des mots de passe. L'attaque est la suivante :

- 1 Le livreur choisit un mot de passe m quelconque et construit le colis c_2 (avec un gâteau empoisonné, mais en utilisant aussi les mêmes cadenas qu'Isabelle utiliserait, en particulier, il utilise le cadenas d'Isabelle pour construire c_1 puisque c'est ce que Bob s'attend à voir). Le colis est ensuite livré à Bob.
- 2 Bob reçoit un colis qu'Isabelle aurait très bien pu faire elle-même, et suit donc le protocole et construit c'_2 en remplaçant le cadenas externe par celui d'Isabelle.
- 3 Le livreur ne peut certes pas ouvrir c'_2 , mais peu importe, il le jette simplement et fabrique c'_1 de zéro, avec une autre boîte, ce qui est possible puisqu'il a choisi lui-même m .
- 4 À la réception de c'_1 , Bob mange le gâteau empoisonné. □

Exercice 7 :

- 1 Bob ouvre un nouveau compte à l'organisation, à un nouveau nom jamais utilisé jusqu'à aujourd'hui — disons *Bobo*. Il reçoit donc une nouvelle clé, et l'organisation est prête à fournir le cadenas de Bobo à qui le demandera.
- 2 Bob envoie ensuite à Isabelle, dans un coffre fermé avec le cadenas de cette dernière, une note indiquant le nom de Bobo.
- 3 Isabelle peut alors obtenir le cadenas de Bobo auprès de l'organisation, et envoie le gâteau à Bob dans un coffre fermé avec ce cadenas (dont Bob a la clé, et dont l'attaquant ne connaît pas le nom du propriétaire).

Solution.

Ce genre de protocole est facilement attaquable en utilisant le principe fondamental. En effet, si le livreur imite *Bob*, cela lui permet de voler le gâteau avec l'attaque suivante :

- 1 Le livreur crée un nouveau compte à l'organisation, appelons-le par exemple *Bobi* ;
- 2 Il donne à Isabelle un coffre fermé avec le cadenas de cette dernière, contenant une note avec le nom “Bobi” à l'intérieur ;
- 3 Isabelle pense que ce nouveau compte est celui de Bob, et fait livrer le gâteau dans un coffre fermé avec le cadenas de Bobi, que le livreur peut donc ouvrir. \square

Exercice 8 :

- 1 Isabelle choisit un long mot de passe et appelle Bob au téléphone pour lui communiquer.
- 2 Isabelle envoie ensuite à Bob un coffre fermé avec le cadenas de ce dernier et contenant le gâteau et le mot de passe convenu écrit sur un papier.
- 3 À la réception du colis, Bob vérifie qu'il contient le mot de passe convenu, et refuse de manger le gâteau sinon.

Solution.

Cette solution est sûre mais *invalidé* : comme expliqué au point 1 p.12, l'utilisation de canaux de communication en dehors du livreur sont interdits. \square

Exercice 9 :

- 1 Isabelle choisit un long mot de passe et l'envoie à son client dans un coffre fermé avec le cadenas de ce dernier.
- 2 Le client (Bob ici) choisit un mot de passe également, l'ajoute dans le colis reçu, et renvoie le tout à Isabelle fermé avec le cadenas de cette dernière.
- 3 Si Isabelle reçoit un colis avec deux mots de passe dont le sien, elle ajoute le gâteau dans le coffre, le ferme avec le cadenas de Bob, et fait livrer le tout.
- 4 À la réception du colis, Bob ne mange le gâteau que s'il y trouve les deux mêmes mots de passe qu'à l'étape 2.

Solution.

Ce protocole est valide. Intuitivement, il est identique à V3, si ce n'est qu'on ajoute au colis un mot de passe choisi par Isabelle, en plus de celui de Bob. Le protocole est donc aussi sûr que V3 et donc accepté pour le phase de conception de l'activité. En revanche, l'absence d'indications d'identité à l'intérieur des boîtes comme dans V4 le rend faible au même type d'attaque que V3, où le livreur commande un gâteau de son côté, empoisonne sa propre commande, et arrive à la faire accepter à Bob. En détails, l'attaque se déroule comme suit :

- 1 Le livreur commande un gâteau à Isabelle, qui choisit un mot de passe m_I et l'envoie au livreur dans un coffre fermé avec le cadenas de ce dernier.
- 2 Quand Bob commande le gâteau à Isabelle, le livreur ne relaie pas sa demande et lui donne en retour un coffre contenant m_I , fermé avec le cadenas de Bob.
- 3 Bob prenant ce colis pour la réponse d'Isabelle, il l'ouvre, y ajoute un mot de passe de son choix m_B , et referme le tout avec le cadenas d'Isabelle.

- 4 Le livreur transmet ce colis à Isabelle, et prétend qu'il s'agit de sa réponse pour sa propre commande. Isabelle ouvre donc le coffre, y trouve m_I et m_B (et pense que m_B est le mot de passe du livreur comme dans l'attaque contre V3), y ajoute le gâteau, et ferme le colis avec le cadenas du livreur.
- 5 On retrouve alors la fin de l'attaque sur V3 : le livreur ouvre son colis, empoisonne le gâteau à l'intérieur, referme le tout avec le cadenas de Bob, et le donne à ce dernier qui y trouve m_I et m_B et mange donc le gâteau empoisonné.

Cette attaque n'est pas fondamentalement plus difficile à comprendre que celle sur V3, mais son nombre substantiellement plus élevé d'étapes peut la rendre un peu (trop) ardue à trouver pour un animateur formé à la cryptographie seulement via ce document. Dans le cadre de cette activité, il est parfaitement acceptable de se satisfaire des propositions visiblement aussi sûres que V3 comme ici, et de ne pas s'embêter outre mesure à chercher ce genre attaques complexes par usurpation d'identité. Présenter V3 à la fin de la phase de conception comme la proposition d'une équipe fictive — et dérouler l'attaque apprise par cœur si le public ne la trouve pas — est largement suffisant. Rappelez-vous simplement que, même si l'attaque en question est trop complexe à trouver pour vous, les protocoles ne contenant aucune information sur les identités à l'intérieur des colis sont a priori attaquables avec un scénario du style “*le livreur et Bob font une commande en parallèle, le livreur fait passer la commande de Bob pour la sienne, ce qui lui permet de l'empoisonner puis de la faire accepter à Bob malgré tout*”. □

Exercice 10 :

- 1 Isabelle écrit sur un papier un mot de passe construit à partir des lettres de son prénom (par exemple, *sleabIle*), le met dans un coffre, avec un gâteau, fermé avec le cadenas de Bob, et fait livrer le tout à ce dernier.
- 2 Quand Bob reçoit le colis, il reconnaît les lettres du nom d'Isabelle et comprend que le colis a été envoyé par cette dernière, et peut donc manger le gâteau.

Solution.

Ce protocole peut être considéré comme valide, mais n'a aucune forme de sécurité. Il repose uniquement sur de la *sécurité par obscurité* (voir point 2 p.12), c'est-à-dire, sur le fait que le livreur ne disposerait pas de la description du protocole — ce qui est faux. Dans le cas présent, le livreur peut aisément empoisonner Bob en lui envoyant un colis fermé avec le cadenas de Bob et contenant un gâteau empoisonné et le message “*sleabIle*”. □