ÉLÉMENT DE PORTFOLIO 03

Autre

1 DÉFINITION DE CET ÉLÉMENT

Titre de l'élément : Recherche en cryptologie et enseignement de la cryptologie.

URL de l'élément :

- `https://isec.sfpn.net`
- `https://crypta.sfpn.net`
- `https://www.dunod.com/sciences-techniques/exercices-et-problemes-cryptographie-0`

2 MOTIVATIONS DU CHOIX DE CET ÉLÉMENT

Depuis sa création et pendant toute la période d'évaluation, l'équipe ALMASTY était une équipe universitaire composée uniquement d'enseignants-chercheurs. En principe, la moitié de notre activité concerne l'enseignement, notamment de la cryptologie, du HPC, de la théorie de la complexité, etc. Les membres de l'équipe ont notamment assumé la responsabilité de cours de cryptologie dispensés en première et en deuxième année du parcours **Sécurité, Fiabilité et Performances** (SFPN) du master informatique de Sorbonne Université. Ces cours, ainsi que les projets d'étudiants que nous encadrons, sont la principale source de discussion au sujet de l'enseignement au sein de l'équipe.

Le premier élément du portfolio de l'équipe ALMASTY illustre déjà comment les problèmes que posent la conception de nos enseignements suggèrent des pistes de recherche. Nous discutons ici du flux d'idées inverse, c'est-à-dire des actions menées par l'équipe pour la formation par la recherche et des développements menés par l'équipe pour moderniser l'enseignement de la cryptologie.

3 PRÉSENTATION DE CET ÉLÉMENT

Les enseignants en cryptographie peuvent s'appuyer sur quelques ouvrages de référence ("*textbook*"). Un petit nombre ont été traduits en français, notamment *Cryptographie, Théorie et pratique* de Douglas Stinson, paru en 2003. Cet ouvrage a légèrement vieilli et il est surtout épuisé. Cependant, pour l'animation de séances de travaux dirigés (TDs) ou de travaux pratiques (TPs), les enseignants sont largement livrés au système D.

3.1 Travaux Dirigés

Un membre de l'équipe a publié en 2012 la première édition de l'ouvrage *Exercices et problèmes de cryptographie* [5]. Cet ouvrage comble un manque en proposant une série d'exercices (corrigés) de cryptologie abordant une large palette de thèmes, allant bien au-delà des grands classiques : sécurité sémantique, modes opératoires pour le chiffrement par blocs, attaques sur des versions réduites de l'AES, construction de SHA-3, cryptanalyse linéaire et différentielle, générateurs pseudo-aléatoires, théorie algorithmique des nombres, attaques sur les chiffrements RSA et Elgamal, sur les signatures de Schnorr et Lamport, etc. Une troisième édition est parue pendant la période d'évaluation (octobre 2018) et une quatrième édition est actuellement en cours d'impression (avec une parution prévue pour juin 2023). Cet ouvrage joue toujours un rôle utile une décennie après sa parution ; il permet en effet d'animer des séances de TDs et il est utilisé dans plusieurs autres universités françaises.

3.2 Travaux Pratiques

Du côté des travaux pratiques, la situation n'est pas meilleure. Une rapide recherche sur internet montre que beaucoup de cours de cryptologie contiennent en fait *peu* de TPs, et que ceux qui existent ne sont ni très passionnants ni très en phase avec la pratique moderne de la cryptographie (sans même parler de la recherche dans ce domaine).

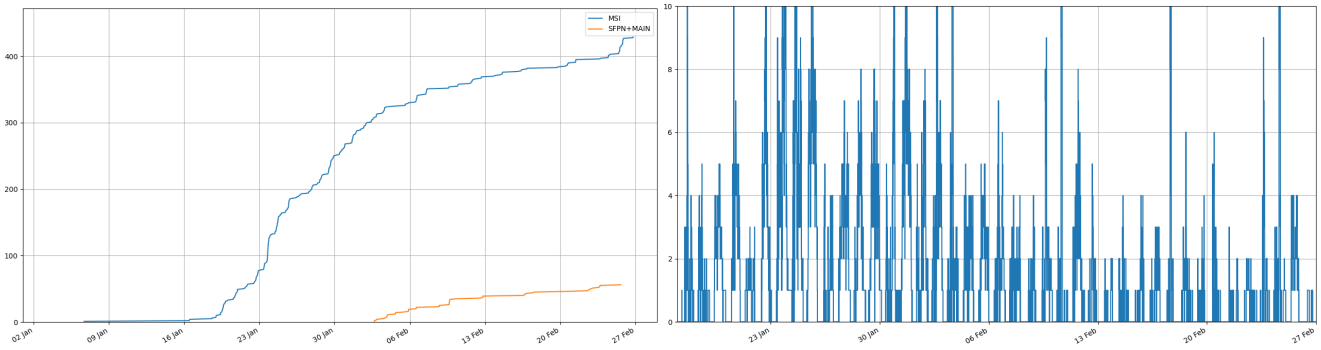

FIGURE 1 – Nombre de tâches réalisés par deux groupes d'étudiants (gauche) et nombre d'étudiants connectés à la plate-forme (droite), en 2023.

Un membre de l'équipe a commencé en 2013-2014 à mettre en place une collection de *web-services* hébergés dans le nuage, avec lesquels les étudiants pouvaient interagir. Non seulement c'est un scénario réaliste d'utilisation de la cryptographie mais cela donne des possibilités pédagogiques inédites :

- Les étudiants peuvent implanter des protocoles cryptographiques (avec le web-service comme « interlocuteur »).
- Les web-services peuvent contenir des secrets cryptographiques. Ceci permet aux étudiants d'implanter des attaques pour tenter de les extraire.

Les étudiants apprécient particulièrement l'aspect interactif : c'est-à-dire que le système leur dit *tout de suite* s'ils ont réussi, et (essaie) de leur expliquer *pourquoi* ils n'ont pas réussi.

Sur le plan de la cryptologie, cela permet de faire accomplir aux étudiants des tâches qui seraient impossibles à mettre en place dans une séance traditionnelle et enrichit considérablement les TPs.

Nous avons choisi de présenter le tout comme un jeu d'aventure rétro en mode texte. Au fur et à mesure que les étudiants résolvent des tâches cryptographiques, ils peuvent explorer une version virtuelle (déserte) de leur campus universitaire et progresser dans le "scénario", qui leur réserve quelques surprises. Il y a même une bande son ! La figure 2 donne une petite idée du résultat.

À très peu d'exceptions près, les étudiants plébiscitent le choix qui consiste à présenter le tout comme une sorte de jeu avec une vague intrigue et une ambiance *geek*. Ils sont nombreux à dire qu'ils apprécient le côté ludique, et « *plus concret* » qu'un TP classique.

Du point de vue des enseignants, il est manifeste que le système capte davantage l'attention des étudiants que des TPs "classiques", comme en témoigne la figure 1. Des étudiants se connectent tous les jours, week-end compris. On voit même des étudiants valider des tâches le samedi à 23h ! Le tout a fait l'objet d'une soumission aux Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information (RESSI) en 2023.

3.3 Formation par la recherche

Cinq des dix doctorants (co-)encadrés par l'équipe sont des étudiants à qui les permanents ont fait cours. C'est une politique, sinon militante, du moins volontariste : nous estimons qu'il est juste que nous prenions en thèse les étudiants que nous formons.

Dans cette optique, nous tenons à ce que nos cours de M2 présentent des résultats récents (nous fixons cette barre à 10 ans). À l'automne 2022, nous avons présenté la spectaculaire cryptanalyse du schéma de signature "post-quantique" Rainbow par W. Beullens qui datait de quelques semaines [1], la signature PICNIC [4] basée sur le "calcul réparti dans la tête" et qui date de 2017, ou encore l'algorithme très simple que nous avons publié l'été dernier pour résoudre des systèmes polynomiaux booléens [2].

Enfin, une de nos publications [3] a débuté par un projet de recherche donné à un binôme d'étudiants de M1. Le binôme a tellement bien réussi que l'une des deux a poursuivi par un stage de recherche au sein de l'équipe, à l'issue duquel la publication a été rédigée. L'étudiante a tourné, pendant un confinement, une vidéo de présentation pour un colloque virtuel, et a fini par rejoindre l'équipe pour préparer son doctorat.

```
[Lower brain functions initialized]

Vous êtes dans un local poubelle.  Il fait tout noir. Il y a des néons au
plafond, mais ils sont éteints.  Seul un éclairage d'urgence de faible
intensité, au niveau du sol, éclaire un peu la pièce.  Le sol et les murs
sont couverts de carrelage, probablement pour faciliter le nettoyage. Une
porte équipée d'une barre anti-panique donne sur une autre pièce.

Ici se trouvent des déchets.
Ici se trouve un conteneur-poubelle.
Ici se trouve une inscription sur le sol.

>>> 
```

```
                                                       UGLIX v4.0 beta
                                                (LPNHE Research Terminal)

                    Active user: charles
```

```
*** Process received signal ***
[UGLIX:04968] Signal: Segmentation fault (11)
[UGLIX:04968] Signal code: Address not mapped (1)
[UGLIX:04968] Failing at address: 0xb)

Dumping core...
[Uglix Secure Vault Enclave]

IV = c0696483ca1898e3296b5af242fe13de
```

```
PTpH9h1JY7wX6S1sexmJahOdyVcLVKiAO4rBSdAeVgRDSMfqtng0B/Z0l2rFa1tN
D53VeMnuiOZhHGylDcU+wIzjuP38968TfNmjdJv0J9F15vGUZ//zSbpJGtCWkEnz
8lqmF7L37gv/BtfWgKUAnS8qdye3mbWKci9nHQiaJUASwXoBHdQUeEOCLoW4pkjz
cuv53CCiCOB2rekxtF2QQI3+1S/EniGh0BHwGBbBcixqZXCug8PIah4zh2KgYJtS
GOqbt4OJBhSwlEHwt+9/aslBMsff8XoUkApxtKTZOuXXgyAgP1bWbxxV32+1LiCr
SL/fXYCTYQi4Jx/vuLJWIM6ggPUemJzkPvSIPbQn+T8MhesL3NRQ6PyEI0IJRUhv
burY9Z/2DMjiF2XdsCK70vdqHjK6WzRACvJ708+FaBShs+OzpeNGNS21B6dFvUvi
GTd0rVxLk/sMFrldm+iAoAOII2N6FVD7+BIamoxvowel6kCwSzkkkafZpKMcNpI/
bZE24LsMfPJ6QAfx8PqEyTpwa/atlKBuQw0bENNndaV2OzzMxd6yQ8OEgVyH97eL
0hYmJ9Pe7GrIrCWIFy8W/TLtzSXsVC6RHffW0E/d+Ld/DQEV73aSLJ3rzur4JMti
634hCmjU6GAAYKVEvZldiMo28Tbw0IOmmP/1IDqkU+DT3xlaxOnDsM6regrTK5In
7cwn3v44ZmjPcbQ50yJvTDAxhmlQy4QNuqsS48eAwNF7WC4AeG+/7oCXMX9cfD6y
yq31YDWLM45fm5Iuo7RY4j0BCHYdRRIu3U1ZAZO0l7a2opK0ap2niJ0/VmjsxT2t
ZcvaSgb10ZMVmKg03kCYSUhVRZu3q+0DC0TR+ZU1ae34gRWj/SLxRN+HsWzBCDRZ
7XGrLaj9ne8g09Vse07u0l+mVuEMsW/myLZ/6QjRAfVswde2VKCJm+cDvI9+RTpl
3DZXEEMXgaHKJQgtaloRfpC9NvEfCLNcq5ShG6B/eKmNWq8J/XFZ/b0Ll+dPy2IG
wQMrsu//Mmx1GoVS/tavk+LhSCQIlcmdi9fxN81bmpq08oImqQGOK09kFhnbO0t8
zy6ELOvYy0EIzTexnUYunqtAtxZrmCD7JavtnG0tSsYq18Vg674jFesfoKAUSYDj
jrcfs4jPWIcBTA1DXaw3XIQfs/NQ+1MXU3XZ8lH1VExc+x5nDfq24mColBsMdfm+
vTWNBrO8q2kOttiXMn94fPeauHbQjeMyyi9wfISzAtQ9IwRDMm38FQH22P6MYERX
goqPHxwG8wLtu/nwNf221lJXxJP0rpf24H4sEclO8NVVyG5nxIbWC2kHRLVJ8B4M
5cMYRCXBkgKmXZp6yGgaGdm0aLZkBHMRgnh5w8NUyLAYR0skPWsD6qtPdvMh1qyX
oREflZMxoNTGtf5nankJKhUzxAyBF4msaQ70i7oBvb//upzHLRjdHulooq6XIutW
JkN4uNzTnURStnCsPq1Rnu5PK+71i/TMy577cJUbcHqxp8aTzib+mjv37rTK/tcI
oxUlCBHHY3JL5yamqP6AQI21JZvCvVqXMQt7vTIgFZQMZg2/goiLF3shgFFGemcZ
OhYY8Rep5XtiqDWt+DelQQ+n2ruOjqQwwPI6Drw9yA1KRBVZ4A7fiJmjz/+EV626
jDWCI3sMubtQRysVqWjZp5i5XGfzTZ30eWvreEEMHY9H1aa5ytkT7ceE7t+Pb1kN
CBg8CRabNgwamuuqC6PMjvjVIk+sfZ4+9xhMPQ4pnjCY/gH2zyc1OCYNAhjpvVqz
musrzQSAXefXe85zrV3V7tc4cjJ6GzeeVraVt7MgmE5/tvAuq5zxS1QvYE0FOGeF
sw2laimMjh5DWp2W7DxC1WInqNbaNSly5UQIFuEA2zZmuNMkDAh1v2WNCVtIZsiA
z6Y3spz6/zZmwWxWVTqbEzEuYDC6RjHCJw4DPVnIrtbriGIRrPuoMDTj5+/TLnuo
Ami1+16OCfaGHgt6n63mfADCvBCHIFkEmnlDw2h5Q1Jbpni5aW1lOSt5ihxtgBBB
```

```
>>> 
```

```
                                                   UGLIX v4.0 beta
                                                 (Lab Director Proxy)

                    Active user: charles

WARNING: - This prototype is INCOMPLETE.
WARNING: - It does not fully implement RSA PKCS#1 v1.5.
WARNING: - Here is what it actually does:
WARNING:   - read the input as a hex-encoded number (big-endian)
WARNING:   - run the IA decision algorithm on the input
WARNING:   - raise it power d modulo N (d is the secret key)
WARNING:   - print the result in hex (big-endian)
WARNING: - This does not produce valid OpenSSL signatures
WARNING:   out of the box because the padding is not applied

YOU HAVE BEEN WARNED

                    Data:                           deadbeef

                    Checking data ...

                    No problem detected

                    Signature:
                    8641ada0857569f020f43f44e4dbe6c5bdacb4fd20ac3ec542edfff10969db0fe31bc61968b58f16e1df7b4d03244764a13f6
f57937810380f9daf69d23359363d09f744e98fd7a8e6ae3aa783a7db76e1d1a776174a4497bf7ecb1754f59b378ef07677d66f354523544e983d386b
038f50673b8eebce1064295af9592844a92e03f41b74e840699496adfae04c46fe9a912ed9fdede646f917daf4598f8fe8d88140fe69c8b66cab7ac29
c086e1ba89c9723675924bf9b9a2ca8c0d5ec63b9d51c8

[press any key]
```

```
Vous êtes dans le hall du bâtiment, au niveau inférieur.  Les murs et le sol
sont peint en rouge pêtant.  Ca fait presque mal aux yeux.  Une cloison vitrée
vous sépare d'une bibliothèque vide au sud.  En levant le nez, vous voyez tous
les étages de couleurs bariolées, ainsi que l'enchevêtrement d'escaliers qui
y conduit.  À ce propos, celui qui vous permettrait de monter au niveau du
dessus a été retiré.  Au Nord, l'espace de restauration est fermé, mais un
couloir jaune donne sur le coin Nord-Est.  Un couloir turquoise débouche côté
Ouest.

Ici se trouve une clef secrète RSA qui traine dans un coin.

>>> 
```

```
                                                UGLIX v4.0 beta
                                               (Service terminal)

Active user: charles
public-key uploaded: YES

                                            PKI menu
                                            --------


0. Query public-key directory
1. Upload public-key
2. Upload signature
3. Tutorial
4. Submit Certificate Signature Request
5. Return to main menu
```

```
Vous êtes dans un petit passage couvert qui sépare deux cours.  Au Sud, une
porte vitrée donne sur le hall d'entrée de la bibliothèque.  En face, au Nord,
une autre porte vitrée, fermée celle-là, donne sur une rotonde qui ceinture
le pied d'une tour peinte en rouge et marquée :

                         ,agd"                 "bg,
                      ,gdP"                      "Ybg,
                    ,dP"                            "Yb,
                  ,dP"                                "Yb,
                 ,8"                                    "8,
                ,8'                                      `8,
               ,8'              d8888  .d8888b.           `8,
               d'              d8P888 d88P  Y88b           `b
                              d8P 888      .d88P
                             d8P  888     8888"
                            d88   888      "Y8b.
                            8888888888888    888
                                  888 Y88b  d88P
               Y,                 888  "Y8888P"            ,P
               `8,                                        ,8'
                `8,                                      ,8'
                 `8a                                    a8'
                  `Yba                                adP'
                    "Yba                             adY"
                      `"Yba,                     ,adP"'
                         `"Y8                  8P"'


>>> sud
Vous êtes dans le hall d'entrée de la bibliothèque des licences.  Vous voyez
l'intérieur à travers les portes vitrées qui vous en séparent : il n'y a personne.
Les portes sont fermées et vous ne pouvez pas entrer.  L'éclairage est tamisé et
les bancs en mousse rouge et mauves sont étonnamment confortables.  Ca vous donne
envie d'y faire une petite sieste, mais le distributeur de friandise à l'Est du
hall fait un bruit désagréable.

Ici se trouve un distributeur de friandises et de gadgets.
Ici se trouve un catalogue électronique.

>>> 
```

```
Vous êtes dans la salle de travail de l'équipe des responsable de la sécurité
informatique.  Un vieux carton de pizza traîne dans un coin.  Il n'y a pas de
fenêtres.

Ici se trouve une spécification du journal des évènements de sécurité (partie II).
Ici se trouve un terminal d'administration du security engine.

>>> look spécification
Le MAC qui accompagne chaque entrée du journal des évènements de sécurité
fait 256 bits.  Il se décompose en fait en 4 blocs de 64 bits chacun :
- le premier (octets [0:8]) est obtenu en évaluant un véritable MAC. Celui-ci
                           [--------REDACTED--------]
- les 3 autres blocs contiennent des parts d'un secret partagé avec le
  système de partage de secret de Shamir.
Plus précisément, si on note :
- p : le nombre 2**64 - 59 (qui est premier),
- X : les bits [0:64] du MAC,
- A : les bits [64:128] du MAC,
- B : les bits [128:192] du MAC,
- C : les bits [192:256] du MAC.
Alors A == R(X) mod p, où R est un polynôme de degré 8 inconnu.
Alors B == S(X) mod p, où S est un polynôme de degré 16 inconnu.
Alors C == T(X) mod p, où T est un polynôme de degré 24 inconnu.
Les coefficients constants de R, S et T sont des "firmware update keys", qui
                           [--------REDACTED--------]
Pour reconstituer ces coefficients, qui sont en fait R(0), S(0) et T(0), on
                           [--------REDACTED--------]
                           [--------REDACTED--------]

>>> 
```

4 RÉFÉRENCES BIBLIOGRAPHIQUES

[1] Ward Beullens. Breaking rainbow takes a weekend on a laptop. In Yevgeniy Dodis and Thomas Shrimpton, editors, *Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part II*, volume 13508 of *Lecture Notes in Computer Science*, pages 464–479. Springer, 2022.

[2] Charles Bouillaguet, Claire Delaplace, and Monika Trimoska. A simple deterministic algorithm for systems of quadratic polynomials over gf(2). In Karl Bringmann and Timothy Chan, editors, *5th Symposium on Simplicity in Algorithms, SOSA@SODA 2022, Virtual Conference, January 10-11, 2022*, pages 285–296. SIAM, 2022.

[3] Charles Bouillaguet, Florette Martinez, and Julia Sauvage. Practical seed-recovery for the PCG pseudo-random number generator. *IACR Trans. Symmetric Cryptol.*, 2020(3) :175–196, 2020.

[4] Melissa Chase, David Derler, Steven Goldfeder, Claudio Orlandi, Sebastian Ramacher, Christian Rechberger, Daniel Slamanig, and Greg Zaverucha. Post-quantum zero-knowledge and signatures from symmetric-key primitives. In Bhavani Thuraisingham, David Evans, Tal Malkin, and Dongyan Xu, editors, *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, Dallas, TX, USA, October 30 - November 03, 2017*, pages 1825–1842. ACM, 2017.

[5] Damien Vergnaud. *Exercices et problèmes de cryptographie — 3ème édition*. Dunod, 2018.