Informatique débranchée : Déchiffrez c'est gagné

Culture Sciences de l'Ingénieur

La Revue 3E.I

Édité le 13/02/2024

école normale supérieure paris-saclay

Anthony JUTON[1]

[1] *Professeur agrégé à l'ENS Paris-Saclay – DER Nikola Tesla*

Cette ressource fait partie du N°111 de La Revue 3EI de janvier 2024.

La ressource « Fondamentaux de la sécurité réseau » [2] présente notamment les principes de chiffrement symétrique et asymétrique. Pour illustrer le cours, parfois un peu théorique, est née cette activité ludique d'informatique débranchée. L'objectif de l'activité est de sensibiliser les étudiants aux mécanismes de communication sur canal non sécurisés en pratiquant un peu de chiffrement par clés symétriques et asymétriques, dans l'esprit du protocole TLS.

L'activité est présentée comme elle a eu lieu en décembre 2023, avec 20 étudiants de Master, pendant le cours de réseau. Des adaptations ou une assistance de l'enseignant sont à prévoir en fonction du niveau en mathématiques des étudiants. Une version 2 est en réflexion pour faire intervenir l'authentification par certificat.

1 - Le contexte et les règles du jeu

Trois équipes de 6/7 étudiants séparées en 2 chiffreurs, 2 déchiffreurs et 2 hackeurs (répartition variable suivant les équipes).

Les chiffreurs doivent faire deviner un mot de 8 lettres reçu dans une enveloppe aux déchiffreurs. Le seul moyen de communication, non sécurisé, est un tableau commun pour tous. Tout le monde joue en même temps. Les calculatrices sont autorisées.

Le premier mot déchiffré vaut 3 points, le deuxième vaut 2 points et le dernier vaut 1 point, qu'il soit déchiffré par l'équipe associée à ce mot ou par le hackeur d'une autre équipe (l'équipe du hackeur obtient alors le ou les points).

Le protocole proposé est inspiré de TLS (le déroulement précis est décrit en partie 4) :

1. Le chiffreur calcule et diffuse une clé publique RSA via le tableau.
2. Le déchiffreur reçoit la clé publique et l'utilise pour chiffrer une clé symétrique créée pour l'occasion (type AES, mais plus simple) et l'envoyer via le tableau.
3. Le chiffreur utilise alors la clé symétrique pour chiffrer le mot à faire deviner et envoie le mot chiffré à ses partenaires via le tableau.
4. Le déchiffreur déchiffre le mot et annonce la réponse.

Pendant ce temps, les hackeurs tentent de craquer les clés privées adverses pour obtenir la clé symétrique, déchiffrer le mot de l'équipe adverse avant elle et obtenir le point.

2 - Le protocole à clé symétrique

TLS utilise le protocole à clé symétrique AES-128 ou AES-256. AES combine des substitutions et des permutations. Pour faire simple et rapide à chiffrer, on utilise uniquement des substitutions, avec un Ou exclusif utilisant une clé symétrique 20 bits.

Les caractères, uniquement des lettres majuscules, sont codés sur 5 bits.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Exemple : coder GEII avec la clé 0xabcde puis déchiffrer le message chiffré avec la même clé.

```
Message GEII      : 00111001010100101001
XOR clé 0xabcde   : 10101011110011011110
Message chiffré   : 10010010100111110111


Message chiffré   : 10010010100111110111
XOR clé 0xabcde   : 10101011110011011110
Message déchiffré : 00111001010100101001
                      G    E    I    I
```

Pour le jeu, on utilise une clé de 20 bits et un algorithme de chiffrement Ou exclusif. Le mot à chiffrer faisant 8 caractères, on concatène la clé avec elle-même pour chiffrer 40 bits.

3 - Le protocole à clés asymétriques RSA

Pour transmettre les clés symétriques, on utilise l'algorithme de chiffrement à clé publique RSA, également utilisé par TLS 1.2 (mais plus par TLS 1.3).

Algorithme à clé publique RSA (du nom de ses inventeurs Rivest, Shamir, Adleman)

- Choisir deux grands nombres premiers p et q (p et q sont normalement des nombres sur 1024 voire 2048 bits).
- Calculer n = p * q et z = (p-1)*(q-1)
- Choisir un nombre d (d<n) tel que d et z n'aient pas de facteur commun
- Trouver e tel que e * d = 1 mod z
- Former des blocs de k bits tels que 2^k<n

- Calculer pour chaque bloc $C=P^e \bmod n$
- Déchiffrer en calculant $P = C^d \bmod n$

{e,n} est la clé publique

{d,n} est la clé privée

C'est réversible : le contraire ({d,n} publique et {e,n} privée) marche aussi

Exemple, p = 3, q = 11, d=7. Chiffrer « ENS ».

Les caractères, uniquement des lettres majuscules, sont codés sur 5 bits.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

On trouve n = 33, z = 20

On choisit d = 7 (7<33 et 7 et 20 n'ont pas de facteur commun)

On trouve e = 3 (3*7 = 21 = 1 mod 20)

On choisit k = 5 ($2^5 = 32 < 33$)

Chaque caractère est un bloc. P = {E,N,S} = {5,14,19}.

On le chiffre avec la clé publique {e,n} = {3,33}

- $E \rightarrow 55^3 \bmod 33 = 26$
- $N \rightarrow 1414^3 \bmod 33 = 5$
- $S \rightarrow 1919^3 \bmod 33 = 28$

Le message transmis sur le canal est donc C = {26,5,28}

On déchiffre avec la clé privée {7, 33}

- $26^7 \bmod 33 = 5 \rightarrow$ E
- $5^7 \bmod 33 = 14 \rightarrow$ N
- $28^7 \bmod 33 = 19 \rightarrow$ S

Le message déchiffré est bien P = {E;N;S}

Pour le jeu, on limite à p<50 et q<50 et on impose k=5 (donc n > 32)

Le site Dcode [3] permet de calculer des clés publiques et privées,de chiffrer des messages et de craquer des petites clés. Il permet également de voir le temps nécessaire à un PC pour craquer la clé privée à partir de la clé publique. Il faut de très (très) grands nombres pour obtenir un temps significatif.

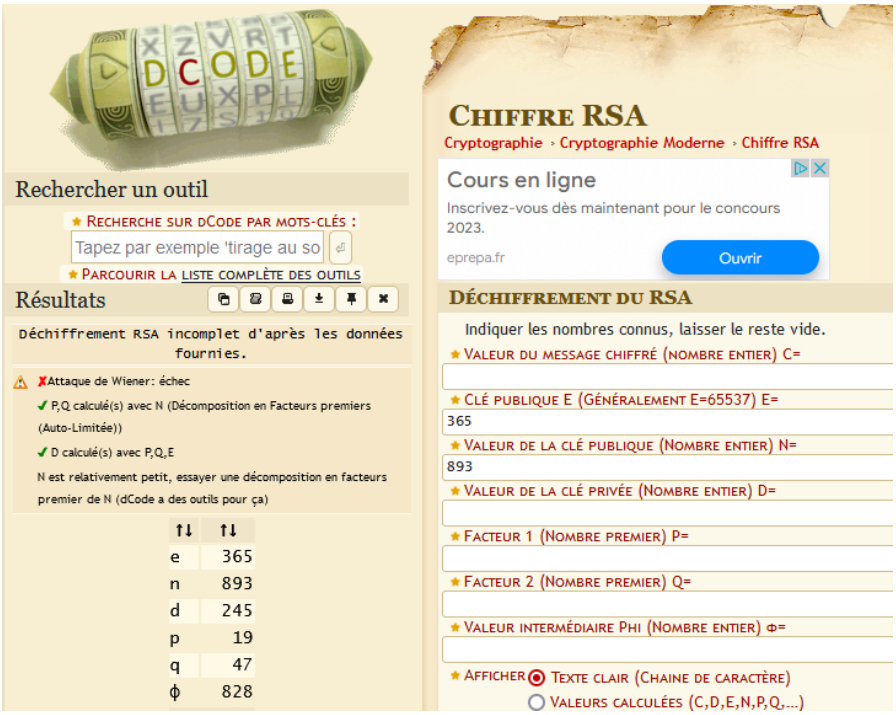


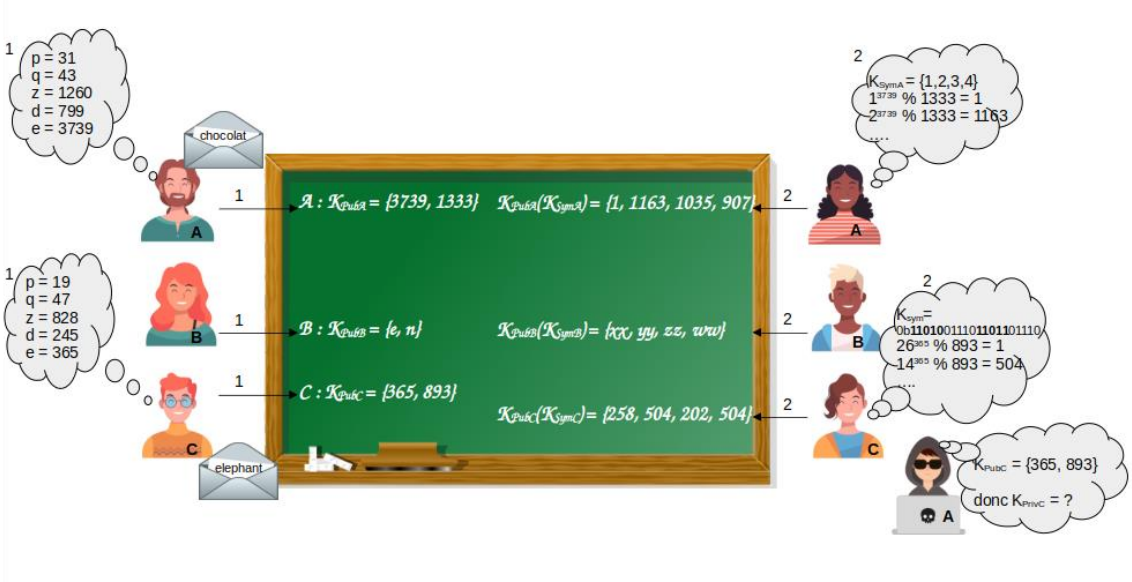
Figure 1 : Copie d'écran du site Dcode > RSA [3]

4 - Déroulement du jeu

Les règles sont expliquées, les étudiants sont répartis entre les chiffreurs d'un côté de la salle avec leur enveloppe et les autres de l'autre côté de la salle.

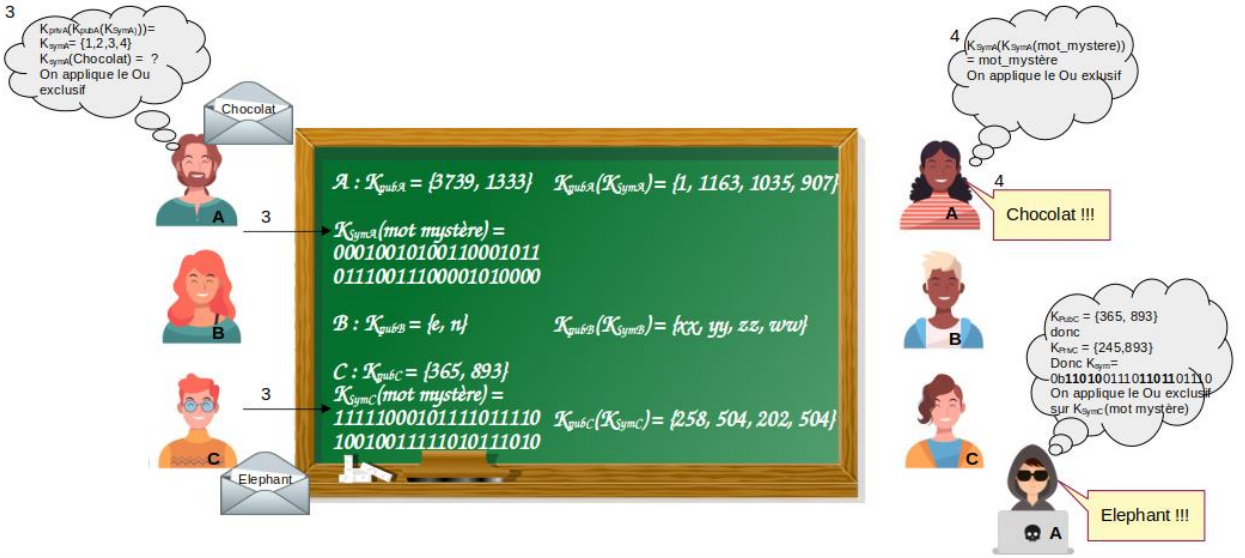
Le tableau est à la vue de tous.

Les chiffreurs doivent trouver un jeu de clés RSA. L'enseignant aide un peu si besoin. Une fois la clé publique obtenue, le chiffreur écrit celle-ci au tableau (1). Les déchiffreurs de son équipe codent alors, avec cette clé publique, la clé symétrique qu'ils ont choisie et écrivent la clé chiffrée au tableau (2). Pendant ce temps les hackeurs des autres équipes cherchent la clé privée pour pouvoir déchiffrer la clé symétrique.



Une fois la clé symétrique chiffrée affichée sur le tableau, le chiffreur la déchiffre avec sa clé privée et l'utilise pour chiffrer le mot mystère puis écrit le mot chiffré au tableau (3). Le déchiffreur utilise la clé symétrique pour déchiffrer le mot mystère et annonce le résultat (4).

Pendant ce temps les hackeurs tentent de trouver les clés privées des chiffrements RSA des autres équipes. S'ils vont suffisamment vite, ils peuvent déchiffrer le message contenant la clé symétrique et ainsi déchiffrer les mots mystère des autres équipes et obtenir leur point.



5 - Conclusion

Les exercices sur les clés symétriques et asymétriques faits pendant le cours, le jeu a duré une petite heure, explication comprise. L'émulation a bien fonctionné, la perspective de gagner quelques chocolats donnant un argument pour tenter de craquer le code de l'équipe adverse. L'équipe A a trouvé le mot A et craqué la clé de l'équipe B, sans avoir le temps de deviner le mot B avant l'équipe B. L'équipe C s'est trompé dans le transfert de sa clé publique et a fini par trouver le mot C avec l'aide de tous. L'enseignant a aidé les uns et les autres pour trouver les clés, chiffrer ou déchiffrer.

Le jeu a permis de mettre en évidence la possibilité de communiquer de manière confidentielle à travers un canal non sécurisé, sans avoir échangé des clés à l'avance. Le fait de s'écarter des ordinateurs a amené les étudiants à prendre la mesure des calculs nécessaires pour le chiffrement symétrique, le chiffrement asymétrique et le craquage d'une clé.

La limite à 50 pour les nombres premiers est sans doute un peu élevée. 40 serait plus raisonnable. Il faudrait peut-être donner une méthode pour trouver d et e.

L'an prochain, un essai d'introduction des certificats avec autorité de confiance est prévu.

Références

[1]: Computer Networks, Andrew Tanenbaum, Nick Feamster, David Wetherall, Pearson Education Limited

[2]: Fondamentaux de la sécurité réseau, M. Sechehaye, A. Juton, février 2024, https://eduscol.education.fr/sti/si-ens-paris-saclay/ressources_pedagogiques/fondamentaux-dela-securite-reseau

[3]: Dcode, Outil pour déchiffrer/chiffrer avec RSA https://www.dcode.fr/chiffre-rsa

[4]: Cybersécurité, Clés publique/privée, Certificat X509, PKI, Chiffrement RSA, fichier .pem OPC-UA, Hervé Discours, https://www.youtube.com/watch?v=58FUQzWxs3Y

Ressource publiée sur Culture Sciences de l'Ingénieur : https://eduscol.education.fr/sti/si-ens-paris-saclay