# CYBERCRYPT: Learn Basic Cryptographic Concepts while Playing

Monir Azraoui, Solenn Brunet, Sébastien Canard, Aïda Diop, Lélia Eveillard, Alicia Filipiak, Adel Hamdi, Flavie Misarsky, Donald Nokam Kuate, Marie Paindavoine, Quentin Santos and Bastien Vialla

Orange Labs - Applied Crypto Group - Caen (France)**
Normandie University - UNICAEN - ENSICAEN - CNRS - GREYC - Caen (France)

**Abstract.** Cryptography is used since the Antiquity to securely transmit messages. Thanks to a key that is shared between parties, the armies have been able to securely send commands and information to a distant unit. In the middle of the Twentieth Century, cryptography has experienced a drastic evolution and has become even more widespread, thanks to the development of computer science and the democratization of the digitization of the data transmitted between people. In particular, cryptologists Whitfield Diffie and Martin Hellman invented in 1976 the concept of public key cryptography, revolutionizing the way data can be protected, and paving the way to a new kind of cryptography that can be used for much more than data confidentiality.

CYBERCRYPT is a collaborative and educational game that allows people to understand basic cryptographic mechanisms. It allows to discover from the oldest techniques (Scytale, Caesar and Vernam's encryption, Enigma machine) to most recent ones, currently implemented in our daily transactions (electronic signature, key exchange, etc.).

CYBERCRYPT allows, through several rich and comprehensive workshops, to discover the different techniques used in cryptography, and also highlights the crucial importance of cryptography to protect our digital daily life.

## 1 Introduction

Today, we welcome a class of 16 14-year-old children, 6 girls and 10 boys. At first, we explain them that every day, they are using cryptography several times during their journey, in their mobile phone, in a computer when they make use of Internet, etc. We next explain that they will play together to the CYBERCRYPT game, which is a collaborative and educational game that will permit them to better understand cryptography. We finally ask them to form two groups of 8

** This work has been done while all the authors where at Orange Labs. Our paths are now mostly parted, although we continue to cross on a few occasions. Today, Monir and Solenn are at the CNIL, Aïda is at Ericsson, Donald is at MasterSecurity Conseil, Marie is at Famoco, Quentin is at TrustInSoft. Lélia and Flavie are studying somewhere. Finally, Sébastien, Alicia, Adel and Bastien are still at Orange Labs.

players. The aim of the game (from a more basic perspective, compare to the educational purpose) is to get a maximum of points. We then explain that, at the end of the 1-hour game, we will compare the scores of both teams to declare the winner.

Let us now follow the first team, composed of 4 girls (Hannah, Juliana, Noémie and Selma) and 4 boys (Antoine, Noé, Robin and Solal).

## 2 Setting Up CYBERCRYPT

At first, we show our new players the game board, which one is shown in Figure 1. We then explain that they have just created a new Web society (called Zamazon, EnTube, Papal, etc. depending on the chosen team piece) that will face off several events from competitors through 3 ages. During the one-hour game (not a minute more), they will have to use cryptographic techniques to fight such events. Moreover, each successful event permits the team to win some points. They start the game with 5 points (and the chosen team piece is put on the corresponding box in the board). Antoine insists to choose "EnTube" that makes him laugh a lot.

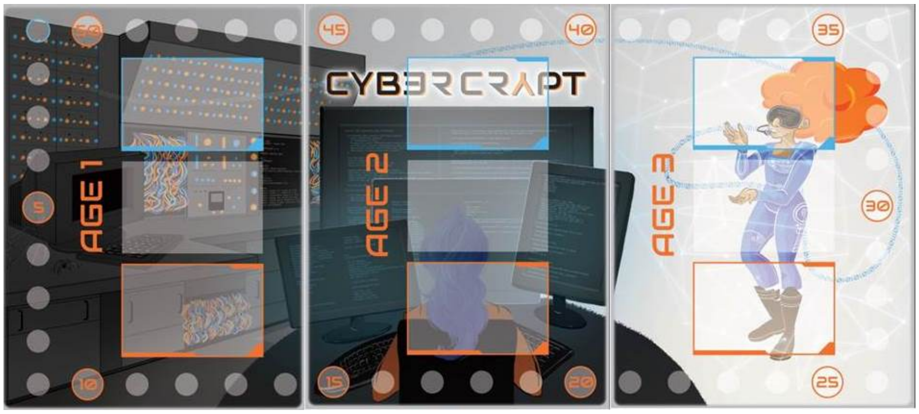


**Fig. 1.** CYBERCRYPT game board

Before starting the game, we finally explain to our new players that there will be three events per age: two are mandatory before being allowed to go to the next age, and the last one is optional. If they choose to go e.g., from Age 1 to Age 2 without having fought the Age 1 optional event, they will not be allowed to come back to this event later. As the game lasts one hour exactly, and as events in Age 3 pay more points, they will have to choose the best strategy to maximize the number of points, and beat the other team!

We present to our players several cards (reverse side, as shown in Figure 2 for Age 1, blue and grey ones being mandatory, and orange one being optional).

They have to choose (without seeing the content) three of them per age. The chosen cards are put (reverse side) in the board, at the right places.

**Fig. 2.** CYBERCRYPT cards

The game can now start. Antoine and Noé tease their friends in the other team: "We will win... Easy-peasy!".

# 3 Age 1

We start the game with the first age.

## 3.1 Playing with Caesar

We first ask Juliana to flip the first card of her choice and she chooses the grey one. The resulting card is shown in Figure 3 (in French language).

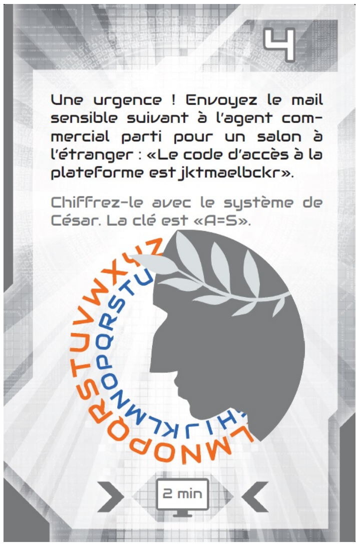
There are in fact three main information in this card:

- the central text explaining the event that the players will have to fight against[1];
- the number of points they will win in case they succeed (top right, here 4 points); and
- at the bottom of the card, the time allotted to resolve the event, here 2 minutes.

In fact, they do not have two minutes to solve the problem. This remains an educational game and the main idea is for players to learn and understand better cryptographic techniques. More precisely, during the time allotted to an event (2 minutes in our case), we, as game masters, do not say anything (except explaining the event itself). At the end of the 2 minutes, we start to help them, but the counterparty is that now they lose 1 point every minute.

We finally give to the team 3 Caesar's wheels (as shown in Figure 4) and the timer is started.

[1] Here, the proposed card says: "An emergency ! Send the following sensitive mail to the commercial agent who has gone abroad for a show: "the access code to the platform is jktmaelbckr". Encrypt it with Caesar's system. The key is A=S."



Une urgence ! Envoyez le mail sensible suivant à l'agent commercial parti pour un salon à l'étranger : «Le code d'accès à la plateforme est jktmaelbckr».

Chiffrez-le avec le système de César. La clé est «A=S».

**Fig. 3.** Caesar card

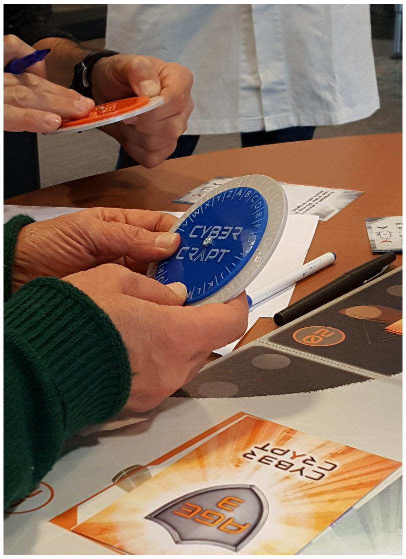
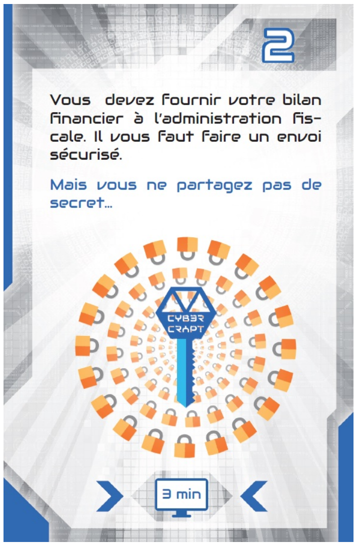


**Fig. 4.** Caesar wheel

In fact, this event is quite easy to manage. During the first age, the aim is primarily to put the players in the mood. Hannah and Selma on one side and Robin on the other side take the lead, each of them with a Caesar's wheel. Selma understands quickly and explains Hannah her idea of putting the letters "A" and "S" in connection in the wheel and starting the encryption of the given message. Robin follows the same idea a few seconds later. Hannah proposes that they start by the end of the message, while Robin, now helped by Noémie and Noé, starts by the beginning. In less than two minutes, they have encrypted the message. The 4 first points are won!

### 3.2 Box and Padlock

It is now the turn of Antoine to flip the next card: the blue one, which is given[2] in Figure 5.



Vous devez fournir votre bilan financier à l'administration fiscale. Il vous faut faire un envoi sécurisé.

Mais vous ne partagez pas de secret...

**Fig. 5.** Box and padlock card

We now give to the team two boxes with two corresponding padlocks, as shown in Figure 6. We split the team into two groups, one playing the EnTube company and the other taking the role of the Tax authority. They now have three minutes to solve the problem.

The idea here is for players to get acquainted with public key cryptography basic principles. The box and padlock correspond to the public key and the key associated to the padlock is the corresponding cryptographic private key. The Tax authority should keep its private key and send the box and padlock to the EnTube company, that puts the message in the box, closes it with the padlock, and sends back the box through “Internet”. As game masters, we here play the role of the hacker trying to open the box, which is infeasible without the key (or

[2] In English, the text is the following: “You must provide your financial statement to the tax authorities. You need to make a secure transfer. But you do not share any secret ...”

**Fig. 6.** Box and padlock

by breaking the box, as proposed by Noé, but this is not the scope of the game ;-)). Eventually, the Tax authority can open the box with the key, and read the message.

After some failed attempts, Juliana, Solal and Selma find the right solution, in two minutes and 51 seconds. Just in time! Two more points for a total of 11 for the moment.

### 3.3 A Strange Message

We now ask the team whether they want to play the optional card, or if they prefer to go to Age 2. They unanimously say that they want to flip the Age 1 orange card, which is done by Hannah, also shown in Figure 7.

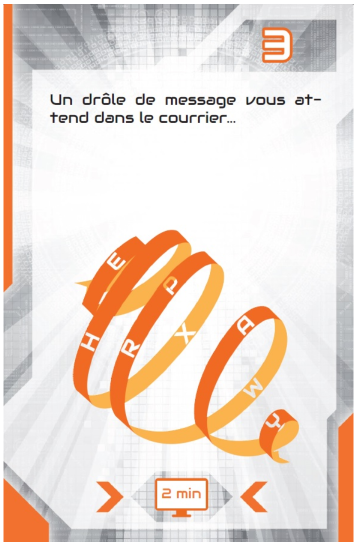
We then give then a strange leather band (see Figure 8 on which they can found letters that seems to have no sense: “MPCAEUEOEROV...”.

In fact, during game installation, we have put on the table two sticks with two different diameters, not saying how they can be useful. We here propose to make use of the Scytale system, which consists in twisting the leather band around the right stick to get acquainted with the received message: “MERCIDEPRENDREC...”[3]. The team beats about the bush with this event, trying first to use Caesar to decrypt the received message. Noémie finally finds the solution and, by chance, tries first the right stick, but after about 2 minutes and a half. According to game rules, they only win 2 points, for a total of 13 points.

## 4 Age 2

We can now proceed to the second age. Twenty minutes have passed since the beginning of the game.

[3] In English, this says “Please contact Fakebook to sell our solution”.



Un drôle de message vous attend dans le courrier...

**Fig. 7.** Strange message's card

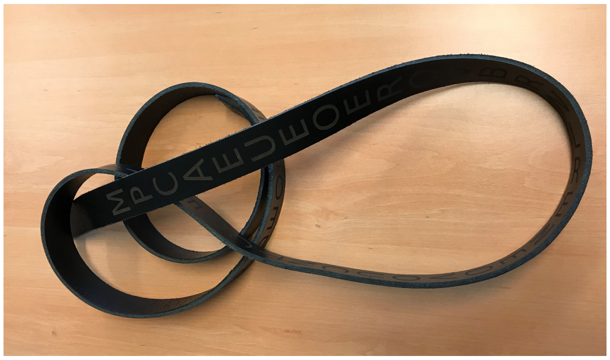
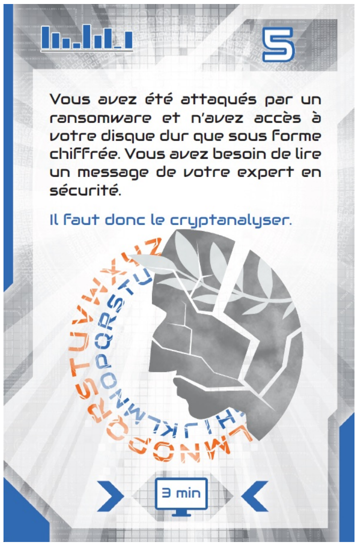


**Fig. 8.** Box and padlock

### 4.1 Breaking Caesar

It's Noémie's turn to flip the next card, and she chooses the blue one, which is shown, in French language[4], in Figure 9. This card has a particularity. On top left, one can see a pictogram. We explain the players that this corresponds to a resource that they can buy to help them in solving this event. It costs them 3 points.

[4] This text can be translated in English as "You have been attacked by a ransomware and you only have access to your hard drive in an encrypted form. You need to read a message from your security expert. It must be cryptanalyzed."



Vous avez été attaqués par un ransomware et n'avez accès à votre disque dur que sous forme chiffrée. Vous avez besoin de lire un message de votre expert en sécurité.

Il faut donc le cryptanalyser.

**Fig. 9.** Breaking Caesar card

We have first to explain the word "ransomware" that nobody knows. As recently there has been such kind of story in the media, it's quite easy.

We finally give them the message to be cryptanalyzed, that started with

"PSVWUYIPIWSVHMREXIYVWUYERX...".

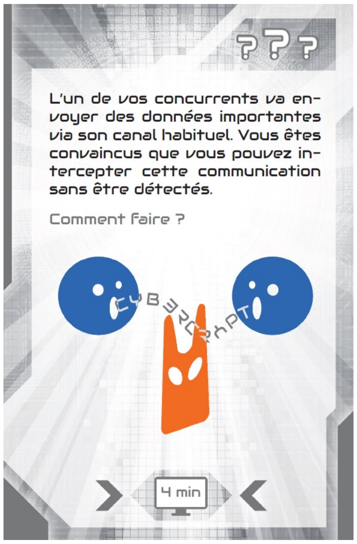
They have 3 minutes to obtain the corresponding plain message. As this is encrypted using Caesar's code, the purpose of this event is to realize a frequency analysis by counting the number of time each letter appears in the text and, with good probability, the most frequent letter corresponds to an "E". Using the Caesar's wheel, it then becomes easy to retrieve the whole text.

In fact, Hannah has this idea quite quickly, remembering that when she has helped Selma to encrypt the message, during Age 1, she was no longer using the wheel (unless rarely) after a few letters. Good idea, the resource is not necessary and they can save the corresponding 3 points!

At first, the team looks disorganized, everybody trying his own tests, and no one really progresses. Eventually, they decide to split them into two groups: Hannah, Antoine, Selma and Noé on one side, and Noémie, Robin, Juliana and Solal on the other side. Each starts to count, until Antoine, watching the text, explains that the letter "W" seems to appear a lot of time. Noé quickly follows the idea of his friend and, with the help of Hannah, they start to decrypt the message. After a small latency, the other group decides to work similarly, starting from the end of the message. They finally succeed but in more than 4 minutes. They only win 3 more points.

### 4.2 Man in the Middle Attack

We then propose to Robin to flip the grey card corresponding to Age 2. The card[5] is given in Figure 10. As game masters, we now play the same game as before with boxes and padlocks, to exchange a message that the players cannot see. They also have access to their own box.



L'un de vos concurrents va envoyer des données importantes via son canal habituel. Vous êtes convaincus que vous pouvez intercepter cette communication sans être détectés.

Comment faire ?

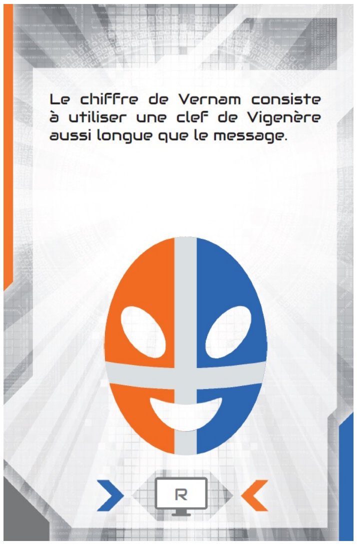
**Fig. 10.** Man in the Middle card

The idea is for them to perform a man-in-the-middle attack, exchanging our box with their own (as nothing identify the fact that this is ours), so that they can obtain the message (using their own key), then put it on our box, and sends it back to us, so that the attack cannot be detected. After several tries, Robin finds the solution and explains to the others how to proceed. They are excited, and Antoine has a look to the other team, trying to show them that they are stronger.

The card that we were exchanging contained the following text: “With Caesar's code, a key as long as the message must be used to obtain a system resistant to the frequency analysis attack”.

Hannah thus remarks that the card does not contain a number of points, by question marks. In fact, they have won the resource card that is shown in Figure 11. We moreover explain them that a resource card finally gives 2 more points at the end of the game. We also explain that this card may be useful later.

[5] The texts says “One of your competitors will send some important data using their usual channel. You are convinced that you can intercept this communication without being detected. How to proceed?”



Le chiffre de Vernam consiste à utiliser une clef de Vigenère aussi longue que le message.

**Fig. 11.** Resource card: Vernam

It remains only 18 minutes before the end of the game and the EnTube team decides to go to Age 3, and not play the optional event. Vigenère will not be played this time.

## 5 Age 3

Age 3 can now start. The team has currently 16 points plus a resource card, and then 18 points.

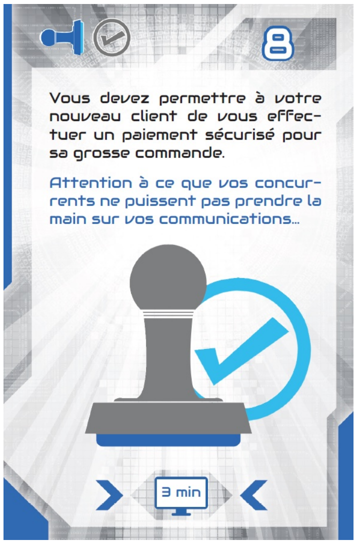
### 5.1 Certification Authority

Noé is the next one to flip the Age 3 blue card, and the result[6] is given in Figure 12. Taking a look at the card, Selma remarks that this event may necessitate the use of a resource card.

We now play the role of the Man-in-the-Middle attacker when the team tries to securely exchange their message. The idea is to call a Certification Authority to certify that the box/padlock is the ownership of the new customer. Again, we split the team into two groups, one playing the customer, and the other the EnTube company.

The whole team tries several things, but we always succeed our attack. They finally accept to buy the resource card, given in Figure 13.

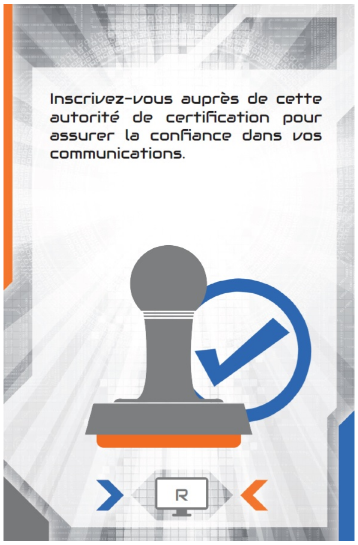
[6] The English translation is “You have to allow your new customer to make a secure payment for his last order. Be careful that your competitors cannot take the control of your communications...”



Vous devez permettre à votre nouveau client de vous effectuer un paiement sécurisé pour sa grosse commande.

Attention à ce que vos concurrents ne puissent pas prendre la main sur vos communications…

**Fig. 12.** Certification authority card



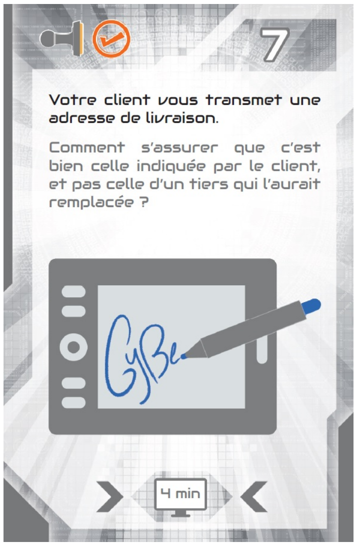
Inscrivez-vous auprès de cette autorité de certification pour assurer la confiance dans vos communications.

**Fig. 13.** CA resource card

We propose to Solal to play the role of the Certification Authority (giving him a special pen), saying to the others that everybody trust Solal and that they can ask him to help them to secure their transmission. After 3 minutes against this event, they have the general idea that Solal has to write something on the box but they do not know exactly what. We then start to help them by saying that there are two important things that should appear on the box: the identity of the owner and something else. Hannah finally finds the solution: Solal has to write on the box "Customer's box" and sign it. Then, if we try to replace such box by our own, this will be detected by the EnTube team, which one should verify the name on the box, and Solal's signature. Man-in-the-Middle attack is no more possible. They have successfully fought against this event, but in 4 minutes and 48 seconds. They obtain 6 points.

### 5.2 Signature

Selma then flips the next card, showed in Figure 14. This event[7] aims at presenting the concept of digital signature.



Votre client vous transmet une adresse de livraison.

Comment s'assurer que c'est bien celle indiquée par le client, et pas celle d'un tiers qui l'aurait remplacée ?

**Fig. 14.** Signature card

We split again the players into two groups, one playing EnTube team and the other playing the role of the customer. Solal is still the Certification Authority, and is given several coloured marks and a blank sticker. We give the message to send to the customer group and, on our side, we play again the role of the bad guy, trying to impersonate the customer by sending a fake address.

After 4 minutes of consideration, the team mainly asks the Certification Authority Solal to do the entire job, and we have to insist that this is not necessarily his role. We then propose them to consider the coloured marks as a

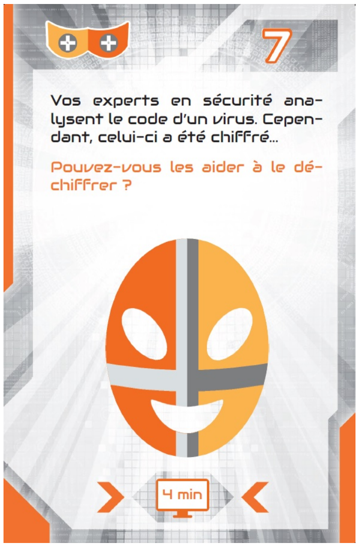
[7] English text corresponds to: "Your customer sends you a delivery address. How to ensure that it is the one indicated by the customer, and that no third party has replaced it?"

way to identify someone, and after a while, we explain that the EnTube company should verify both that the content of the message can be verified and that it comes from the right actor (through Solal). This helps them a lot and they finally give the right way to proceed: Solal signs, using the blank sticker, the information that the yellow mark corresponds to the customer, and the latter can use a yellow mark to "sign" the message to send. Both the sticker and the signed message are then put on the box and EnTube can verify both conditions.

The team has been a little bit longer than expected and only obtains 5 points. But it remains them 7 minutes to try the last orange card.

### 5.3 Vernam cryptosystem

Solal is the last one to flip the card (see Figure 15), which explains that they have to decrypt a message[8].



Vos experts en sécurité analysent le code d'un virus. Cependant, celui-ci a été chiffré...

Pouvez-vous les aider à le déchiffrer ?

**Fig. 15.** Vernam card

We then give to the team the message to be decrypted:

"DSUWONRZCSXDILGYQNPHLPKUJXVJAMVLYGPJG"

and the corresponding key

"KSHDYTNELSPROANQBCHDUAKDHTIQPMALNCVSG".

[8] The text says that "Your security experts analyse a virus code. However, it has been encrypted. Can you help them to decrypt it?"

Using Caesar's wheel, this is an easy but quite burdensome work to perform. This exactly shows how the Vernam system can be fastidious in practice. After a short time of observation (fatigue makes itself felt), Selma decides to take the lead and to organize the team. The message is decrypted but they only win 6 points out of the 7 possible.

## 6 Conclusion of the Game

The EnTube team has finally won a total of 35 points. We take a look at the other table: they obtain only 26 points. Our team has won! Antoine and Noé provoke their classmates in the other team: "Easy-peasy we said".

It is now the time to conclude, and to explain better what is the link between the game they have just played, and the real-world. We detail how their browser is securely connected to servers when they use Internet, using something close to boxes, padlocks and keys. We also explain that current secret key cryptography is in particular an ingenious combination of the Scytale system and Vernam's code.

We finally show to the whole class our reproduction of Enigma (see Figure 16, the famous cryptographic machine that has been used during World War II by the German army. We explain that it corresponds to something similar to the Vernam system they have just played with before, but with some kind of "mechanical" key. We also explain how the real machine worked, and how our own machine is a hybrid one. In fact, the rotors are really connected to the keyboard, and really turn with each other, but the right light is activated by a computer taking as input the key that is pressed, and the rotors' position, and outputting the real Enigma's letter to be switched on. Some of them have recently seen the "Imitation game" movie. They are happy to better understand what is behind this strange machine.

This CYBERCRYPT session is over. They looks very happy. We may have opened new vocations...

## Acknowledgments

This paper has been accepted for the exposition track of HistoCrypt 2019[9].

Many people have participated to the CYBERCRYPT project and this is quite complicated not to forget someone.

This is a joint work between the GREYC research lab in digital science, located in Caen (France) and Orange Labs in Caen (France). CYBERCRYPT has won the Prix Musée Schlumberger in 2017 for the "Têtes Chercheuse" competition, that is organized each year by Relais d'sciences on behalf of the Fondation Musée Schlumberger. This work would not have been possible without their help.

We thank Julien Clément and Loïck Lhote from the GREYC lab, Sylvain Garnavault, François Millet from Relais d'sciences, and also Laurent Mandonnet

[9] `https://www.histocrypt.org/`

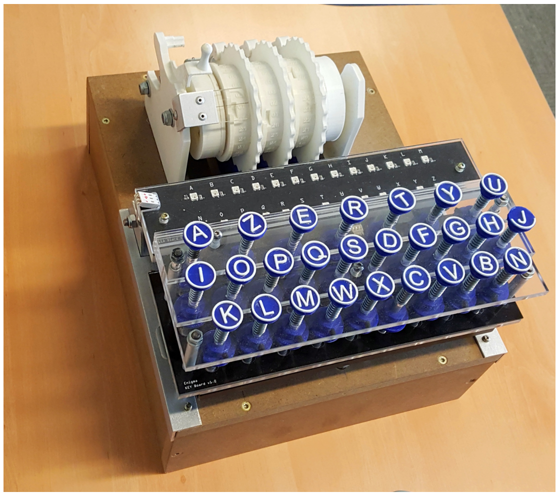


**Fig. 16.** Enigma machine

(for the Enigma machine) and Jean-François Hamon (for the card design) for their help.

Hannah, Juliana, Noémie, Selma, Antoine, Noé, Robin and Solal do not really exist but we certainly have to thank all the children and adults that have accepted to play our CYBERCRYPT game. They have certainly participated to the improvement of our ideas, and the adjustment of all the little details that make our game what it is today.