Gestão de Identidade

I – Alfabeto Secreto

Proposta de Jogo Didáctico para Sensibilização sobre Segurança

Esta actividade tem como objectivo sensibilizar as crianças (11-12 anos) para alguns aspectos da segurança, nomeadamente como garantir a confidencialidade da informação trocada em ambientes potencialmente hostis, tais como redes sociais, emails, forae, chats, etc...

A actividade é para ser realizada em grupo, numa aula, ou atelier de tempos livres.

A Ana e o Bruno são amigos e gostam de trocar mensagens sem que ninguém presente na sala possa perceber o que estão a dizer um ao outro.

Para isso, combinam entre si uma forma de escrever mensagens que ninguém mais possa perceber: escrevem tudo num **alfabeto secreto** que torna o texto incompreensível para quem não conheça o **segredo**.

Assim, Ana e Bruno encontram-se num local onde não haja ninguém por perto, e combinam o seguinte segredo:

"Em vez de escrever as palavras normalmente, vamos utilizar um código secreto! Vamos trocar cada letra da mensagem por uma outra, deslocando o alfabeto um certo número de posições para a direita".

Como indicado neste exemplo:

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
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Neste caso, o segredo combinado entre Ana e Bruno foi o número 3, já que o alfabeto secreto corresponde a uma deslocação de 3 posições para a direita do alfabeto original. Esta operação designa-se por encriptação.

Assim por exemplo, as palavras (texto em claro):

"**alfabeto secreto**"

transformam-se em (texto encriptado):

"**doidehwr vhfuhwr**".

Para voltar ao texto original, faz-se a operação inversa, ou seja, desloca-se cada letra do texto secreto 3 posições para a esquerda: o "d" dá um "a", o "o" dá um "l", e assim de seguida. Esta operação designa-se por desencriptação.

O mais engraçado, é que a Ana e o Bruno podem combinar um segredo diferente para cada dia da semana, por exemplo na 2ª feira é 2, na 3ª 3, na 4ª 4 na 5ª 5 e na 6ª 6, ou outros quaisquer que queiram imaginar, desde que sejam compreendidos entre 1 e 25. Têm assim 25 segredos diferentes que podem utilizar.

No decorrer da actividade, os alunos poderão formar grupos de 2, escolhendo um colega com o qual irão trocar mensagens (Ana e Bruno).

A actividade poderá ter o seguinte encadeamento:

1. Ana e Bruno combinam o segredo que irão utilizar, que mais ninguém deve conhecer, devendo para isso sair da sala por breves instantes.
2. A Ana encripta uma mensagem secreta para o seu correspondente.
3. A Ana envia a mensagem a Bruno, fazendo-a passar pelos seus colegas, que a podem ler, sem obviamente entender o seu significado.
4. Bruno recebe a mensagem secreta e utilizando o segredo que combinou com a Ana, desencripta o seu conteúdo.
5. Bruno responde a Ana utilizando o mesmo alfabeto secreto.
6. Etc...

Para ajudar na escrita das mensagens secretas, os alunos poderão utilizar pequenas aplicações on-line, como por exemplo:

http://cryptoclub.org/tools/caesar_cipher.php

http://inventwithpython.com/cipherwheel/

Para perceber até que ponto esta forma de trocar mensagens secretas é válida, a actividade prossegue depois com exploração do Problema do Segredo.

Para Ana e Bruno combinarem um segredo que mais ninguém conheça, tiveram de sair da sala por momentos. E o que acontece se Ana e Bruno não puderem sair da sala? Como vão poder trocar o segredo?

O resto da sessão poderá ser preenchido com os alunos a tentar imaginar soluções para este problema.

A descoberta de uma possível solução poderá ser objecto de uma outra actividade: **Partilha de Segredo**.

Gestão de Identidade

II - Partilha de Segredo

Proposta de Jogo Didáctico para Sensibilização sobre Segurança

A

Esta actividade tem como objectivo sensibilizar as crianças (11-12 anos) para alguns aspectos da segurança, nomeadamente como garantir a confidencialidade da informação trocada em ambientes potencialmente hostis, tais como redes sociais, emails, forae, chats, etc...

A actividade é para ser realizada em grupo, numa aula, ou atelier de tempos livres.

Desta vez a Ana e o Bruno vão aprender uma forma de partilhar um segredo à frente dos seus colegas, sem terem a necessidade de o fazer num local isolado.

Para isso, vão utilizar um "truque", que permite a cada um deles chegar a um número secreto sem nunca o dizer directamente um ao outro, trocando duas mensagens que todos na sala podem ler.

Isto parece impossível, ou então um daqueles truques de magia que depois tem uma explicação de que ninguém estava à espera...

Esse "truque" tem um nome: é conhecido pela troca de segredo de Diffie-Hellman, e é muito utilizado para garantir segurança na Internet. Vamos então ver como funciona!

Em frente de todos os seus colegas, a Ana e o Bruno combinam utilizar dois "números mágicos", que têm uma relação especial entre eles (que explicaremos aos mais curiosos no final da sessão) mas que por agora iremos só chamar a **base** e o **módulo**.

Para efeitos de exemplo, iremos supor que a Ana e o Bruno combinam em frente de todos os colegas que a **base** será o número **5** e o **módulo** o número **23**.

Base: g = 7

Módulo: m = 23

Seguidamente, a Ana e o Bruno escolhem cada um deles um número secreto, que guardam para eles e não dizem a ninguém. Para este exemplo convém que esses números não sejam zero e sejam inferiores a 10.

Assim por exemplo, vamos supor que a Ana escolhe o valor secreto (ou chave privada) 5, e o Bruno escolhe o valor secreto (ou chave privada) 8.

Número secreto da Ana: a = 9

Número secreto do Bruno: b = 8.

Aqui temos de utilizar uma calculadora ou uma pequena aplicação no telemóvel que seja capaz de fazer alguns cálculos matemáticos simples, que seria muito complicado fazer à mão.

Assim, utilizando a calculadora, a Ana calcula o seguinte valor **A** (a sua chave pública):

$A = g^a \bmod m$ ou seja: g levantado à potência a, módulo m.

Por seu lado, Bruno calcula a sua chave pública **B** usando uma outra calculadora semelhante:

$B = g^b \bmod m$ ou seja: g levantado à potência b, módulo m

Neste exemplo, iremos ter:

A = $7^9 \bmod 23$ **= 15**

B = $7^8 \bmod 23$ **= 12**

De seguida, Ana e Bruno enviam um ao outro as suas chaves públicas A e B, sem necessitar de os esconder, podendo dizê-las em voz alta ou escreve-las num papel e fazê-las passar um ao outro pelos seus colegas. **Mas nunca deverão dar a conhecer os números secretos a e b** que serviram para calcular A e B!

Assim, Ana recebe a chave pública B enviada por Bruno (12), e Bruno a chave pública A enviado por Ana (15).

A partir destes valores recebidos, Ana e Bruno irão finalmente poder calcular o segredo.

Assim, Ana calcula:

S = $B^a \bmod m = 12^9 \bmod 23$ **= 4**

Bruno calcula:

S = $A^b \bmod m$ **=** $15^8 \bmod 23$ **= 4**

Ana e Bruno chegaram **exactamente ao mesmo valor secreto**, que neste caso é o número **4**, sem nunca terem falado um com o outro, tendo apenas trocado publicamente valores a partir dos quais ninguém é capaz de deduzir o segredo, pois não conhecem os números secretos que cada um deles escolheu!

No decorrer da actividade, os alunos poderão formar grupos de 2, escolhendo um colega com o qual irão realizar a partilha do segredo (Ana e Bruno).

A actividade poderá ter o seguinte encadeamento:

1. Ana e Bruno combinam os números mágicos **g** e **m** que irão utilizar, em frente dos outros colegas, ou enviando passando uma mensagem em claro pelos seus colegas (na

realidade existem inúmeros pares de números deste tipo que podem ser utilizados por vários grupos).

2. A Ana escolhe um número secreto **a** e calcula a chave pública **A** que envia ao Bruno da mesma forma, numa mensagem em claro.
3. O Bruno escolhe um número secreto **b** e calcula a chave pública **B** que envia à Ana da mesma forma.
4. Ana recebe a chave pública **B** do Bruno e calcula o segredo **S**.
5. Bruno recebe a chave pública **A** de Ana e calcula o segredo **S**.
6. Agora a Ana e o Bruno já podem comunicar usando o alfabeto mágico da sessão anterior e o segredo **S** ao qual chegaram nesta sessão.
7. Etc...

O resto da sessão poderá ser preenchido com explicações dos professores sobre a troca de Diffie-Hellman, e da forma como é utilizada na Internet para garantir a privacidade dos utilizadores.