Universidade da Beira Interior
Faculdade de Engenharia
Departamento de Informática

Segurança Informática
Guia para Aula Laboratorial 2
1º Ciclo em Engenharia Informática
1º Ciclo em Informática Web
1º Ciclo em Matemática e Aplicações

Computer Security
Guide for Laboratory Class 2
B.Sc. in Computer Science and Engineering
B.Sc. in Web Informatics
B.Sc. in Mathematics and Applications

Sumário
Exercícios de exploração do OpenSSL. Utilização da ferramenta OpenSSL para cifrar e decifrar um ficheiro de texto com uma cifra simétrica contínua moderna.

Summary
Exercises for exploring OpenSSL. Utilization of OpenSSL to encrypt and decrypt a text file with a more recent symmetric-key stream cipher.

Pré-requisitos:
Algumas das tarefas propostas a seguir requerem o uso de *software* para efetuar cálculos e o acesso a um sistema que disponibilize a ferramenta OpenSSL. Sugere-se, assim, o uso de uma distribuição comum de Linux, onde todas estas condições estarão provavelmente preenchidas.

1 Exploração do OpenSSL
Exploring OpenSSL

Nesta e nas próximas aulas, o OpenSSL revelar-se-á um recurso extremamente útil no contexto da utilização e estudo de ferramentas criptográficas, entre outras. As próximas tarefas estão desenhadas de forma a explorar, ainda que de forma superficial, este recurso. Este conhecimento será aprofundado ao longo de vários guias.

Tarefa 1 *Task 1*

Inicie o seu computador em sistema operativo Fedora e abra um *browser*. Use a Internet para responder à seguinte questão. **Q1.: O que é o OpenSSL?**

_____

_____

_____

Q2.: Procure saber se o OpenSSL é importante nos dias de hoje e se, apesar de ser um recurso que tem a ver com a segunça da informação, foi a base de alguma vulnerabilidade crítica nos últimos tempos.

☐ O OpenSSL? E isso existe?
☐ O OpenSSL é importante mas não há nada a reportar acerca de bugs severos, em termos de segurança, na sua implementação.
☐ O OpenSSL é muito importante e (eishh!) continha um mega *bug* que ía acabando com a Internet.

Procure continuar a responder acertadamente recorrendo agora ao manual do OpenSSL.
Q3.: Como é que normalmente se pode aceder ao manual de um comando Linux ou Unix *like*?
☐ Não faço a mínima ideia.
☐ Procurando o manual do sistema operativo na gaveta, e abrindo-o na página relativa ao comando.
☐ Escrevendo `$ __________` no terminal...

Q4.: Há alguma diferença entre OpenSSL (devidamente capitalizado) e `openssl` (em `monospace`)?
☐ Sim, há... um é um _____ e o outro é um _____.
☐ *Nope*... as duas designações referem-se exatamente à mesma *toolkit*.

Q5.: Pode usar o OpenSSL para gerar chaves assimétricas?
☐ Nunca experimentei, mas penso que sim.

☐ Nunca experimentei, mas penso que não.

Q6.: Pode usar esta ferramenta para lidar com e-mail cifrado?
☐ Claro. ☐ Não.

Q7.: E para gerar *timestamps*?
☐ Também dá. ☐ Não.

Q8.: E para verificar o MD5 de determinado ficheiro?
☐ FAZ TUDO! ☐ Não, não dá...

Q9.: Pode usar o OpenSSL para fazer o pequeno almoço?
☐ Dá, e pergunta como queremos os ovos.
☐ Não, mas de resto faz tudo...

Tarefa 2 *Task 2*

Construa o comando OpenSSL que lhe permite gerar **10 bytes** aleatórios de qualidade em hexadecimal.

_____

_____

Tarefa 3 *Task 3*

Na linha de comandos (terminal), escreva `openssl` e prima `enter`. **Q10.: Acha que ainda está na linha de comandos?**
☐ Sim. ☐ Não.

Justifique. _____

_____

Escreva `help` na *shell* que deve ter disponível depois do passo anterior. **Q11.: Acha que `help` é um comando/opção do OpenSSL?**
☐ Sim. ☐ Não.

Q12.: Quantos são os comandos principais (*standard*) que tem à disposição?

☐ 1	☐ 45	☐ 46	☐ 47
☐ πr^2	☐ 50	☐ 101110_2	☐ $2E_{16}$
☐ 101111_2	☐ 30_{16}	☐ 1201_3	☐ 48
☐ 110000_2	☐ $2F_{16}$	☐ 1210_3	☐ 49

Q13.: Das seguintes, quais correspondem a opções existentes para o comando `openssl enc`?

☐ -in <file>	☐ -out <file>	☐ -pass <arg>
☐ -e	☐ -d	☐ -a/-base64
☐ -α	☐ -r	☐ -45 <file>
☐ -k	☐ -kfile	☐ -md
☐ -S	☐ -K/-iv	☐ -[pP]
☐ -bufsize <n>	☐ -nopad	☐ -breakfast

Nota: para responder a esta questão, experimentou escrever `enc -help`?

Q14.: Será que o OpenSSL também consegue comprimir e descomprimir ficheiros?
☐ Só não fala como as pessoas!
☐ Não, visto que mesmo o encadeamento de comandos `$ man enc | grep compress` não devolve qualquer resultado...

2 Cifra Simétrica Contínua – ChaCha20

Symmetric Stream Cipher – ChaCha20

O guia laboratorial anterior convidou-o(a) a enveredar por uma *viagem* através das cifras clássicas mais conhecidas. Nesta parte do guia, e após ter explorado um pouco a ferramenta `openssl`, vai experimentar uma cifra da criptografia moderna, para na próxima aula tentar uma implementação muito simples de uma destas primitivas.

A ChaCha20 é uma modificação de uma outra cifra desenvolvida por *Daniel J. Bernstein*. **Q15.: Qual o nome dessa cifra inicial?**
☐ Bachata20 ☐ Merengue20 ☐ Mambo N. 5
☐ Kizomba20 ☐ Salsa20

Tarefa 4 *Task 4*

Abra um terminal na sua máquina com sistema operativo Linux, crie a diretoria `Lab-2` e, lá dentro, coloque o ficheiro `plaintext.txt`. O conteúdo do ficheiro deve ser o nome do(a) seu(ua) colega do lado, bem como duas das suas qualidades e dois **dos seus defeitos**. Demonstre respeito. **Não mostre** o que escrever no ficheiro ao(à) colega.

Use a ferramenta `OpenSSL` para cifrar o ficheiro com a cifra ChaCha20, usando a chave de cifra `abcdefg0123456789`. Para facilitar, o comando para conseguir o objetivo enunciado é dado:

```
$ openssl enc -chacha20 -e -K
abcdefg0123456789 -in plaintext.txt -out
ciphertext.cc20
```

Q16.: A chave de cifra fornecida parece-lhe boa?
☐ Sim, parece.

☐ Não, porque me parece ter pouca entropia.
☐ Não, porque me parece ter muita entropia.

Q17.: O comando funcionou sem problemas?
☐ Sim, funcionou. :D ☐ Não, não funcionou. :(

Q18.: Já verificou o que está dentro do ficheiro?
☐ Sim, já verifiquei usando `$ cat ciphertext.cc20` e o que lá encontrei não faz sentido nenhum.
☐ Sim, já verifiquei e o que lá encontrei faz todo o sentido.
☐ Não, ainda não verifiquei, mas penso verificar já de seguida.

Q19.: Nos espaços incluídos em baixo, coloque a opção que especifica cada parte do comando `OpenSSL` incluído antes.

___ Especifica que o valor incluído a seguir é a chave de cifra em hexadecimal.
___ Especifica que o valor incluído a seguir é a chave de cifra em ASCII.
___ Especifica que o valor incluído a seguir é o nome do ficheiro de saída.
___ Especifica que o valor incluído a seguir é o nome do ficheiro de entrada.
___ Especifica que se trata da operação de cifra (*encryption*).

Tarefa 5 *Task 5*

Mude o nome do ficheiro `ciphertext.cc20`. Dê-lhe o primeiro e o último nome do colega para o(a) qual apontou defeitos e qualidades. E.g., se o colega é o Xico Esperto, dê-lhe o nome de `Xico_Esperto.cc20`. Envie o ficheiro ao(à) colega por *mail* ou por *pen*.

Tarefa 6 *Task 6*

Decifre o ficheiro que recebeu do colega que escreveu sobre si.

Q20.: Qual o comando `OpenSSL` que utilizou?

_____

_____

_____

Q21.: <u>Para além do ficheiro</u>, precisou de pedir ou receber do(a) seu(ua) colega mais algum dado para executar esta tarefa com sucesso?
☐ Não, não precisei.
☐ Sim, precisei, nomeadamente da _____.
☐ Sim, precisei, nomeadamente do ficheiro `plaintext.txt`.

O ChaCha20 é um algoritmo de cifra (de qualquer coisa) simétrica contínua. **Q22.: Ao que é que se refere a palavra *simétrica* nesta designação?**
☐ Ao facto da mesma chave de cifra ser usada para cifrar e para decifrar.
☐ Ao facto da chave de cifra ser usada apenas para cifrar.
☐ Ao facto do algoritmo de cifra ser igual ao algoritmo de decifra.
☐ Ao facto do algoritmo de cifra ser diferente do algoritmo de decifra.

Q23.: É verdade que a ChaCha20 é usada/suportada no OpenSSH?
☐ Sim, é verdade. ☐ Não, é balela.

Q24.: Qual o tamanho máximo que uma mensagem pode ter para que a sua cifra ainda possa ser considerada segura com a ChaCha20?
☐ 100MB ☐ 200GB ☐ 256GiB
☐ 10MB ☐ 1Tebibyte

A RC4 é uma cifra moderna e do mesmo tipo que a Salsa20, mas que é já desencorajada devido à evolução da tecnologia. Foi muito utilizada no *HyperText Transfer Protocol Secure* (HTTPS) e noutras aplicações ou protocolos criptográficos. O seu peso histórico é considerável.

Q25.: O que significa RC4?

R _____ C _____ 4

Q26.: Em que protocolo muito conhecido e usado no passado, para além do HTTPS, é que a RC4 era a <u>única</u> cifra suportada?
☐ No *Speedy González* (SG).
☐ No *Wired Equivalent Privacy* (WEP).
☐ No *Internet Protocol Security* (IPSec).

Caso queira testar a utilização do RC4 com o OpenSSL em versões superiores à 3.0, terá de adicionar ao comando a opção `-provider legacy`. Considere refazer a parte dois deste guia com a RC4.