

A Web Page

https://

Título

4

Ano: [Todos](#) Semestre: [Todos](#) Disciplina: [Todas](#) Época: [Todas](#)

1

2

[Disciplina 1](#)

[Disciplina 2](#)

[Disciplina 3](#)

[Disciplina 4](#)

novo enunciado

3

1

Em todas as páginas estará sempre visível os filtros. Para alterar a pesquisa, basta clicar num dos links e escolher a opção

2

De forma a organizar, aparecerá as disciplinas onde o docente tem enunciados criados. Podemos, mais à frente, adicionar mais informação visível, como por exemplo, nº de enunciados

3

Botão para criar um novo enunciado

4

Indicador se a aplicação está online ou offline

A Web Page

https://

Título

Ano: [Todos](#) Semestre: [Todos](#) Disciplina: [Disciplina 1](#) Época: [Todas](#)

Ano	Semestre	Época	Nome	Rascunho	Público	
2019	Inverno	Normal	Nome 1	false	true	
2019	Inverno	Recurso	Nome 2	false	true	
2019	Inverno	Especial	Nome 3	false	true	
2019	Verão	Normal	Nome 4	false	true	
2020	Verão	Normal	Nome 5	false	false	

1

Caso o enunciado seja público ou se o mesmo já foi disponibilizado, só se poderá consultar. Caso contrário, editar

novo enunciado

Pode vir a ser necessário adicionar mais colunas com informação relativa ao enunciado.

Para *mobile*, pode ser necessário esconder colunas

A Web Page

https://

Título

1

Ano: [2019](#) Semestre: [Todos](#) Disciplina: [Disciplina 1](#) Época: [Todas](#)

Semestre	Disciplina	Época	Nome	Rascunho	Público	
Inverno	Disciplina 1	Normal	Nome 1	false	true	
Inverno	Disciplina 1	Recurso	Nome 2	false	true	
Inverno	Disciplina 1	Especial	Nome 3	false	true	
Verão	Disciplina 2	Normal	Nome 4	false	true	

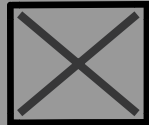
1

Para cada filtro que esteja selecionado, não faz sentido mostrar na listagem, essa coluna

novo enunciado



https://



Título



Ano: 2019

Semestre: Todos

Disciplina: Disciplina 1

Época: Todas

Novo enunciado

Nome

--

Ano

Anos



Semestre

Semestres	▼
-----------	---



Disciplina

Disciplinas



Época

Épocas



Tipo de enunciado

Tipos



Só é possível adicionar novos anos, semestres, disciplinas e épocas se o utilizador estiver *online*

✕ Fechar

 Adicionar

A Web Page

https://

Nome do enunciado

Ano: 2020Semestre: VerãoDisciplina: Disciplina 1Época: Normal

Detalhe

Cabeçalho

Visualizar

1. (1)

Qual a motivação para os esquemas MAC (*Message Authentication Code*), dado que os esquemas de cifra simétrica já fornecem confidencialidade?

2. (1)

Com o objectivo de eliminar o problema do modo ECB quanto à passagem de padrões do texto em claro para o texto cifrado, foi definido o seguinte modo de operação:

$m = m_1, \dots, m_L$ a divisão da mensagem m nos blocos m_i .

R é um número aleatório.

Este modo de operação cumpre o objectivo?

3. (2)

Considere a biblioteca JCA [1]:

3.1

Porque razão a classe 'Cipher' possui o método **update**? Normalmente, a mesma função não podia ser obtida através da utilização repetida do método **doFinal**?

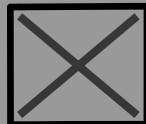
Referências

1

http://www.java.com



https://



Nome do enunciado



Ano: 2020 Semestre: Verão Disciplina: Disciplina 1 Época: Normal







1. (1) Qual a necessidade para os esquemas MAC (Message Authentication Code), dado que os esquemas de cifra simétrica já fornecem confidencialidade?

2. (1) Com o **Detalhe:** Permite editar os metadados do enunciado. Nome, Datas, Rascunho, Público, etc.

Cabeçalho: Permite editar o cabeçalho do enunciado. Estabelecimento de ensino, disciplinas, descrição, etc.

Visualizar: Permite visualizar o enunciado sem ser em modo de edição

- $m =$

- Ré

Este modo de operação custa mais caro, certo?

3. (2) Considere as seguintes afirmações relativas ao enunciado.

As 2 setas servirão para ordenar a pergunta relativamente ao enunciado.

No caso do icon "3 pontos", abrirá uma janela onde o utilizador poderá alterar os dados relativos à pergunta em questão. Se é numérica ou bullet, qual a cotação, caso seja uma pergunta principal, se tem um texto de footer, e bem como eliminar a mesma

3.1 | Por

Normalmente, a mesma função

Para adicionar novas perguntas, o docente terá apenas de inserir a pergunta na caixa de texto e clicar no icon "+".
Terá que posteriormente preencher os campos ponto 2.

metodo do Final?

Referências

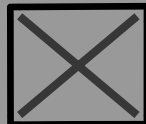
1 <http://www.java.com>

_____ +





https://



Nome do enunciado



Ano: 2020 Semestre: Verão Disciplina: Disciplina 1 Época: Normal





Ao clicar no "Detalhe"

Detalhe

Nome	Nome do enunciado
------	-------------------

Ano	2019	▼
-----	------	---



Semestre Verão

+


Disciplina	Disciplina 1	▼
------------	--------------	---

Época Normal ▼ +


+

Data publicação 01 / 03 / 2020



Data disponibilização 02 / 03 / 2020 



Data entrega 



Duração **150**

Rascunho 

Público 

Tipo	Exame	▼
------	-------	---

✕ Fechar

 Gravar

Referências

1 <http://www.java.com>

A Web Page

https://

Nome do enunciado

Ao clicar no "Cabeçalho"

Ano: 2020 Semestre: Verão Disciplina: Disciplina 1 Época: Normal

Detalhe

Cabeçalho

Visualizar

Instituto Superior de Engenharia de Lisboa

Licenciatura em Engenharia Informática e de Computadores

Disciplina 1

Exame, Primeira Época, Semestre de Verão, 19/20

Duração: 2 horas e 30 minutos

1. (1) Qual a motivação para os esquemas MAC (*Message Authentication Code*), dado que os esquemas de cifra simétrica já fornecem confidencialidade?

2. (1) Com o objectivo de eliminar o problema do modo ECB quanto à passagem de padrões do texto em claro para o texto cifrado, foi definido o seguinte modo de operação:

$m = m_1, \dots, m_L$ a divisão da mensagem m nos blocos m_i .

R é um número aleatório.

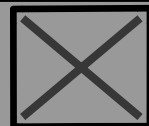
Este modo de operação cumpre o objectivo?

3. (2) Considere a biblioteca JCA [1]:

3.1 Porque razão a classe 'Cipher' possui o método `update`? Normalmente, a mesma função não podia ser obtida através da utilização repetida do método `doFinal`?



https://



Nome do enunciado



Ano: 2020 Semestre: Verão Disciplina: Disciplina 1 Época: Normal





1. (1) Qual a motivação para os esquemas MAC (*Message Authentication Code*), dado que os esquemas de cifra simétrica já fornecem confidencialidade?



2. (1)	Com o objectivo de eliminar a operação:	Detalhe da pergunta	seguinte modo de
--------	---	----------------------------	------------------



- $m = m_1, \dots, m_L$ a divisão

Tipo

Númerica



Número

3

- R é um número aleatório

Cotação

2

Texto de Rodapé

Este modo de operação cu

3. (2) Considerare a biblioteca JCA

3.1 | Porque razão a classe 'Cipher' possui o método `update`? Normalmente, a mesma função não podia ser obtida através da utilização repetida do método `doFinal`?

Referências

1

http://www.java.com





https://



Nome do enunciado



Ano: 2020 Semestre: Verão Disciplina: Disciplina 1 Época: Normal

[i](#) [☰](#) [👁](#)
Detalhe Cabeçalho Visualizar

1. (1) Qual a motivação para os esquemas MAC (*Message Authentication Code*) dado que os esquemas de cifra simétrica já fornecem confidencialidade?



2. (1) Com o objectivo de eliminar o problema da interpretação dos padrões do texto em claro para o texto cifrado, foi definido o seguinte modo de operação:

- $m = m_1, \dots, m_L$ a divisão da mensagem
- R é um número aleatório.

☐ *Itálico*
☐ **Negrito**

☐ *"superscript"*
☐ *"subscript"*

☐

▲ ▼ ■ ■ ■

A Escolher

Este modo de operação cumpre o objectivo?

3. (2) Considerare a biblioteca JCA [1]:



3.1 | Porque razão a classe 'Cipher' possui o método `update`? Normalmente, a mesma função não podia ser obtida através da utilização repetida do método `doFinal`?



Referências

1 <http://www.java.com>

