

**ESCOLA
SUPERIOR
DE TECNOLOGIA
E GESTÃO**

P.PORTO

Criptografia Aplicada
Introdução

Apresentação

- Docente
- Turma
- Disciplina
- Regras Gerais

Apresentação

ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO
POLITÉCNICO DO PORTO

Docente

- Gonalo Hermenegildo
- CV:
 - Licenciatura em Engenharia de Sistemas e Informtica (UM)
 - Ps-graduao em Engenharia de Aplicaes Empresariais (ISEP)
 - Formao em Gesto de Projetos PMI, CMMI, ISO27001, CISSP, COBIT5, CSM, AWS...
 - Previously:
 - Head of Security @ LOQR,
 - Product Manager & Especialista PKI @ AET Europe
 - Project & Team Manager @ Multicert
 - Projetos nacionais e internacionais
 - GRC, AppSec, SOC, PKI, Carto de Cidado, Passaporte Eletrnico, Voto Eletrnico, ID-Porten, smart cards (ITI), E2E...

14/02/2025 GJH @ Criptografia Aplicada 2025.01 4

ESCOLA SUPERIOR DE TECNOLOGIA E GESTO
POLITÉCNICO DO PORTO

Turma

- Chamo-me ...
- Moro em ...
- Continuo nesta licenciatura porque ...
- Espero que esta disciplina ...

28/02/2024 GJH @ Criptografia Aplicada 2024.01 6

ESCOLA SUPERIOR DE TECNOLOGIA E GESTO
POLITÉCNICO DO PORTO

Disciplina

- Cifras simtricas
- Cifras assimtricas (Criptografia de Chave Pblica)
- Funes de disperso (hash) criptogrficas
- Assinaturas digitais e Cdigos de Autenticao de Mensagens
- Autenticao e controlo de acessos
- Certificados digitais e infraestruturas de chave pblica
- Standards criptogrficos
- (Dependente do ritmo):
 - Criptografia Quntica, Ps-Quntica

28/02/2024 GJH @ Criptografia Aplicada 2024.01 7

ESCOLA SUPERIOR DE TECNOLOGIA E GESTO
POLITÉCNICO DO PORTO

Avaliao

- Contnua
 - 1 teste terico (50%)
 - Nota mnima 8 valores
 - 80% parte terica + 20% parte prtica
 - 1 trabalho prtico (50%)
 - 5 Componentes
 - Nota mnima 8 valores
- Exame Final
 - Questes sobre componente
 - Terica (60%)
 - Prtica (40%)

14/02/2025 GJH @ Criptografia Aplicada 2025.01 8

ESCOLA SUPERIOR DE TECNOLOGIA E GESTO
POLITÉCNICO DO PORTO

Regras gerais

- REGRA #1: Devem participar ativamente na aula...
- REGRA #2: No perturbar restantes colegas
- REGRA #3: Telemveis sem som...
- REGRA #4: Devem pesquisar info. relacionada...
- REGRA #5: ...

14/02/2025 GJH @ Criptografia Aplicada 2025.01 9

ESCOLA SUPERIOR DE TECNOLOGIA E GESTO
POLITÉCNICO DO PORTO

Relacionado

Fim

- [Website down ...](#)
- [Hundreds of organizations ...](#)
- [Weak encryption ...](#)

14/02/2025 GJH @ Criptografia Aplicada 2025.01 10

Docente

- Gonçalo Hermenegildo
- CV:
 - Licenciatura em Engenharia de Sistemas e Informática (UM)
 - Pós-graduação em Engenharia de Aplicações Empresariais (ISEP)
 - Formação em Gestão de Projetos PMI, CMMI, ISO27001, CISSP, COBIT5, CSM, AWS...
 - Previously:
 - Head of Security @ LOQR,
 - Product Manager & Especialista PKI @ AET Europe
 - Project & Team Manager @ Multicert
 - Projetos nacionais e internacionais
 - GRC, AppSec, SOC, PKI, Cartão de Cidadão, Passaporte Eletrónico, Voto Eletrónico, ID-Porten, smart cards (ITI), E2E...

Docente

- Responsável por...
 - Aulas Teóricas / Práticas Laboratoriais
- Contacto
 - gjh@estg.ipp.pt
- Horário de atendimento:
 - 6ª das 16h45 às 18h45
 - Notificação prévia (>24h)

Turma

- Chamo-me ...
- Moro em ...
- Continuo nesta licenciatura porque ...
- Espero que esta disciplina ...

Disciplina

- Cifras simétricas
- Cifras assimétricas (Criptografia de Chave Pública)
- Funções de dispersão (hash) criptográficas
- Assinaturas digitais e Códigos de Autenticação de Mensagens
- Autenticação e controlo de acessos
- Certificados digitais e infraestruturas de chave pública
- Standards criptográficos
- (Dependente do ritmo):
 - Criptografia Quântica, Pós-Quântica

Avaliação

- Contínua
 - 1 teste teórico (50%)
 - Nota mínima 8 valores
 - 80% parte teórica + 20% parte prática
 - 1 trabalho prático (50%)
 - 5 Componentes
 - Nota mínima 8 valores
- Exame Final
 - Questões sobre componente
 - Teórica (60%)
 - Prática (40%)

Regras gerais

- REGRA #1: Devem participar ativamente na aula...
- REGRA #2: Não perturbar restantes colegas
- REGRA #3: Telemóveis sem som...
- REGRA #4: Devem pesquisar info. relacionada...
- REGRA #5: ...

Relacionado

Fim

- [Website down ...](#)
- [Hundreds of organizations ...](#)
- [Weak encryption ...](#)