

# Présentation des protocoles RSAES-OAEP et RSASSA-PSS

## M2 MIC - Cryptographie asymétrique

Jérémie Nekam et Daniel Resende



Mardi 24 octobre 2017

## 1 Introduction

## 1 Introduction

## 2 RSAES-OAEP

- OAEP
- EM-OAEP : Utilisation d'OAEP avec RSA
- Sécurité du protocole

## 1 Introduction

## 2 RSAES-OAEP

- OAEP
- EM-OAEP : Utilisation d'OAEP avec RSA
- Sécurité du protocole

## 3 RSASSA-PSS

- PSS
- Utilisation de PSS avec RSA
- Sécurité du protocole

## 1 Introduction

## 2 RSAES-OAEP

- OAEP
- EM-OAEP : Utilisation d'OAEP avec RSA
- Sécurité du protocole

## 3 RSASSA-PSS

- PSS
- Utilisation de PSS avec RSA
- Sécurité du protocole

## 4 Conclusion

- 1 Introduction
- 2 RSAES-OEAP
- 3 RSASSA-PSS
- 4 Conclusion

Deux protocoles pour deux utilisations différentes :

Deux protocoles pour deux utilisations différentes :

**RSAES-OAEP** Protocole de chiffrement



Deux protocoles pour deux utilisations différentes :

**RSAES-OAEP** Protocole de chiffrement

**RSASSA-PSS** Protocole de signature

## 1 Introduction

## 2 RSAES-OEAP

- OAEP
- EM-OAEP : Utilisation d'OAEP avec RSA
- Sécurité du protocole

## 3 RSASSA-PSS

## 4 Conclusion

Le protocole RSAES-OAEP se décompose en deux parties :

- EM-OAEP
- RSAEP (resp. RSADP) pour le chiffrement (resp. déchiffrement)

# Le schéma OAEP standard

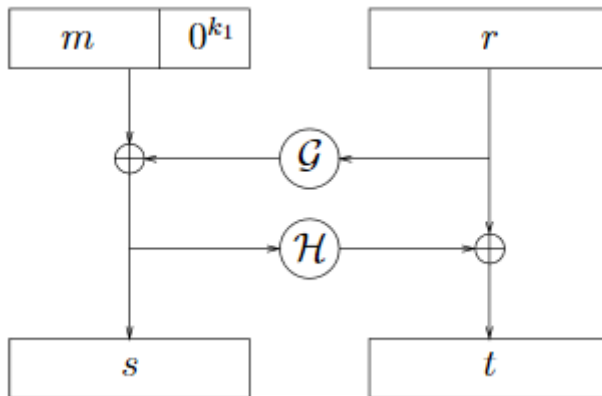


Figure – OAEP

# Le schéma EM-OAEP

Entrées du schéma :

**Hash** Données spécifiant la fonction de hachage

**M** Message

**PS** Padding

**Seed** Aléa

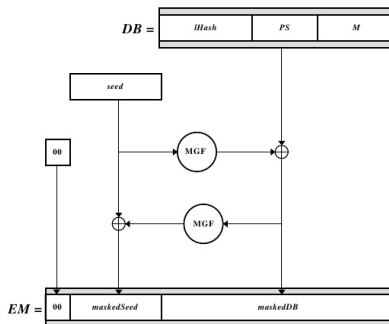


Figure – OAEP



## 1 Introduction

## 2 RSAES-OEAP

## 3 RSASSA-PSS

- PSS
- Utilisation de PSS avec RSA
- Sécurité du protocole

## 4 Conclusion











# Sommaire

- 1 Introduction
- 2 RSAES-OEAP
- 3 RSASSA-PSS
- 4 Conclusion**



# Bibliographie

-  RSA Laboratory.  
Pkcs 1 v2.2 : Rsa cryptography standard.  
2000.
-  RSA Laboratory.  
Rsaes-oaep encryption scheme.  
2000.