Présentation des protocoles RSAES-OAEP et RSASSA-PSS

M2 MIC - Cryptographie asymétrique

Jérémie Nekam et Daniel Resende

Mardi 24 octobre 2017

Sommaire

1 Introduction

Sommaire

1. Introduction
2. RSAES-OEAP
   - OAEP
   - Utilisation d'OAEP avec RSA
   - Sécurité du protocole

Sommaire

1. Introduction
2. RSAES-OEAP
   - OAEP
   - Utilisation d'OAEP avec RSA
   - Sécurité du protocole
3. RSASSA-PSS
   - PSS
   - Utilisation de PSS avec RSA
   - Sécurité du protocole

Sommaire

1. Introduction
2. RSAES-OEAP
   - OAEP
   - Utilisation d'OAEP avec RSA
   - Sécurité du protocole
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

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

Sommaire

1. Introduction
2. RSAES-OEAP
   - OAEP
   - Utilisation d'OAEP avec RSA
   - Sécurité du protocole
3. RSASSA-PSS
4. Conclusion

Schéma de OAEP

Sommaire

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