From Public-Key Cryptography to PKI: Reflections on Standardizing the RSA Algorithm

Jim Bidzos and Burt Kaliski, Verisign

2nd ZKProof Standards Workshop

April 12, 2019
RSA Public-Key Cryptosystem: Review

Key Pairs
• Public key: \((n, e)\)
• Private key: \((n, d)\)
  • where modulus \(n\) is product of two large primes \(p, q\), and exponents \(e, d\) satisfy \(e \cdot d \equiv 1 \mod \text{lcm}(p-1,q-1)\)

Public-Key Cryptosystem
• Encryption of message \(m\) with public key: \(c = m^e \mod n\)
• Decryption of ciphertext \(c\) with private key: \(m = c^d \mod n\)

Digital Signature Scheme
• Signature on message \(m\) with private key: \(s = m^d \mod n\)
• Verification of signature \(s\) (and recovery of \(m\)) with public key: \(m = s^e \mod n\)
“The Public-Key Cryptography Standards are specifications produced by RSA Laboratories in cooperation with secure systems developers worldwide for the purpose of accelerating the deployment of public-key cryptography.”
(PKCS #1 v2.2, 2016 [RFC8017])
Outline

• Part I: RSA Signatures
• Part II: RSA Encryption
• Part III: Lessons Learned
Part I: RSA Signatures
RSA Signatures: Original Model
Diffie-Hellman (1976) and RSA (1978)
RSA Signatures: “Standard” Model
PKCS #1 (1991)
How Did Original Model Change to Standard?

1. Hash-then-sign paradigm
2. Partial domain “digests”
3. Algorithm identifiers
4. Fixed padding
5. Block type
6. Encrypting with private key
7. Encrypted digest
1. Hash-then-Sign Paradigm

Message

Digest

00 01 FF ... FF 00 <algID> <digest>

Encrypt

Private Key

Encrypted Digest
2. Partial Domain “Digests”

```
00 01 FF ... FF 00 <algID> <digest>
```

Message

Digest

Encrypt

Private Key

Encrypted Digest
3. Algorithm Identifier

Message

- Digest
  - 0001 FF ... FF 00 <algID> <digest>

Encrypt

- Private Key

Encrypted Digest
4. Fixed Padding

Message

Digest

<algID>

<digest>

Encrypt

Private Key

Encrypted Digest
5. Block Type

Message

Digest

Encrypt

Private Key

Encrypted Digest

00 01 FF ... FF 00 <algID> <digest>
6. Encrypting with Private Key

Message

Digest

00 01 FF ... FF 00 <algID> <digest>

Encrypt

Private Key

Encrypted Digest
7. Encrypted Digest

![Diagram of the Encrypted Digest process]

- **Message**
  - 00 01 FF ... FF 00 `<algID>` `<digest>`
- **Digest**
- **Encrypt**
  - **Private Key**
- **Encrypted Digest**
PKCS RSA Signatures: Summary

Message

Digest

00 01 FF ... FF 00 <algID> <digest>

Encrypt

Private Key

Encrypted Digest
Part II: RSA Encryption
RSA Encryption: Original Model

Diffie-Hellman (1976) and RSA (1978)
RSA Encryption: “Standard” Model
PKCS #1 and #7 (1991)
How Did Original Model Change to Standard?

1. Encrypt-then-wrap paradigm
2. Partial domain encryption keys
3. Random padding
4. Block type
1. Encrypt-then-Wrap Paradigm

```
Message

Encrypt

<random nonzero>

Symmetric Key

Encrypt

Public Key

Encrypted Key

Ciphertext
```
2. Partial Domain Encryption Keys

![Diagram of encryption process]

- **Message**
  - **Encrypt**
  - **Symmetric Key**
  - **Public Key**
  - **Encrypted Key**
  - **Ciphertext**
3. Random Padding

Message

Encrypt

Symmetric Key

Public Key

Encrypted Key

Ciphertext

00 02 <random nonzero> 00 <key>
4. Block Type

Message

Encrypt

Symmetric Key

<random nonzero>

Encrypt

Public Key

Encrypted Key

Ciphertext
PKCS RSA Encryption: Summary

1. Message
2. Encrypt
   - <random nonzero>
   - <key>
3. Encrypt
   - Public Key
4. Encrypted Key
5. Ciphertext

- PKCS RSA Encryption: 00 02 00 00
- Symmetric Key
Conclusion: Five Lessons Learned about Standardizing Cryptography
Five Lessons Learned about Standardizing Cryptography

1. Start with a well-balanced paradigm
2. Develop and improve building blocks
3. Watch for “connection” issues
4. Check for changes in assumptions
5. Review and repeat
1. Start with a Well-Balanced Paradigm

1. Start with a well-balanced paradigm

2. Develop and improve building blocks

3. Watch for “connection” issues

4. Check for changes in assumptions

5. Review and repeat
2. Develop and Improve Building Blocks

1. Start with a well-balanced paradigm
5. Review and repeat
2. Develop and improve building blocks
4. Check for changes in assumptions
3. Watch for "connection" issues
3. Watch for “Connection” Issues

1. Start with a well-balanced paradigm

2. Develop and improve building blocks

3. Watch for “connection” issues

4. Check for changes in assumptions

5. Review and repeat
4. Check for Changes in Assumptions

1. Start with a well-balanced paradigm

2. Develop and improve building blocks

3. Watch for “connection” issues

4. Check for changes in assumptions

5. Review and repeat
5. Review and Repeat

1. Start with a well-balanced paradigm

2. Develop and improve building blocks

3. Watch for “connection” issues

4. Check for changes in assumptions

5. Review and repeat
Questions?
Appendix:
Other RSA Standardization Issues
(overview)
Other RSA Standardization Issues

Public / private key pairs
- Modulus size
- Public exponent values
- Key pair (and prime) generation
- Public key validity
- Public key syntax
- Private key syntax

Message syntax
- Signed messages
- Enveloped (encrypted) messages

Key management
- Certificate syntax
- Certificate request syntax
- Certificate revocation list syntax
- Certificate lifecycle management
- Certificate status protocols
- Private key containers

Cryptographic APIs and more …
Selected References for Further Reading
Research References (1)


Research References (2)


Standards References


Special thanks to Chris Mitchell for helpful feedback on early history of public-key standards and access to additional publications, and to John Linn for perspective on the development of Privacy-Enhanced Mail.