Cryptography 101: From Theory to Practice

Chapter 12 – Key Establishment

Rolf Oppliger

March 17, 2022

Terms of Use

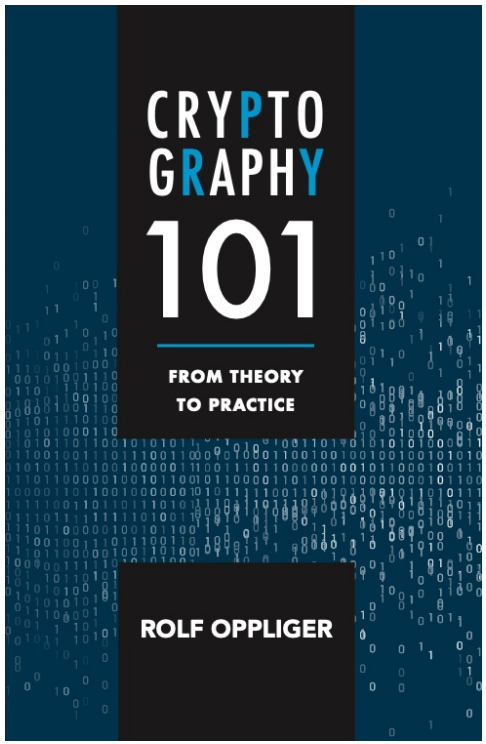
- This work is published with a CC BY-ND 4.0 license ()
  - CC = Creative Commons ()
  - BY = Attribution ()
  - ND = No Derivatives ()

whoami

rolf-oppliger.ch
rolf-oppliger.com

- Swiss National Cyber Security Centre NCSC (scientific employee)
- eSECURITY Technologies Rolf Oppliger (founder and owner)
- University of Zurich (adjunct professor)
- Artech House (author and series editor for information security and privacy)

Reference Book



ISBN 978-1-63081-846-3

`https://books.esecurity.ch/crypto101.html`

Challenge Me

Part III

PUBLIC KEY CRYPTOSYSTEMS

Outline

12. Key Establishment

1 Introduction
2 Cryptographic Systems
3 Random Generators
4 Random Functions
5 One-Way Functions
6 Cryptographic Hash Functions
7 Pseudorandom Generators
8 Pseudorandom Functions
9 Symmetric Encryption
10 Message Authentication
11 Authenticated Encryption

13 Asymmetric Encryption
14 Digital Signatures
15 Zero-Knowledge Proofs of Knowledge
16 Key Management
17 Summary
18 Outlook

12. Key Establishment

12.1 Introduction
12.2 Key Distribution
12.3 Key Agreement
12.4 Quantum Cryptography
12.4 Final Remarks

12. Key Establishment

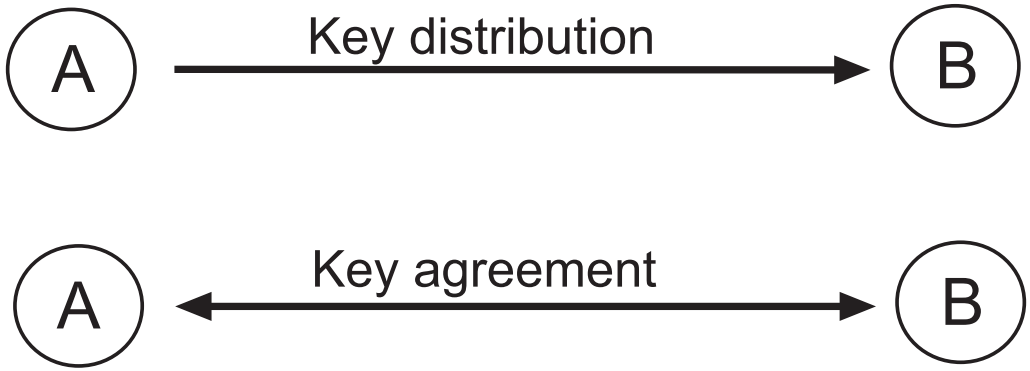
12.1 Introduction

- The establishment of keys is a major problem in secret key cryptography
- It represents the Achilles' heel for its large-scale deployment
- Two approaches
  - Key distribution center (KDC), such as Kerberos
  - Key establishment protocols

12. Key Establishment

12.1 Introduction

- Types of key establishment
  - Key distribution
  - Key agreement (aka key exchange)



12. Key Establishment

12.2 Key Distribution — Merkle's puzzles

- In 1975, Ralph C. Merkle proposed an idea that predates (but is conceptually similar to) public key cryptography
- It is theoretically interesting but not practical

Table 12.1
Merkle's puzzles

A		B
(n)		(n)
Generate $P_i = (i, k_i)$ for $i = 1, \ldots, n$ Permute $P_1, \ldots, P_n$		
	$\xrightarrow{P_{\pi(1)}, \ldots, P_{\pi(n)}}$	
		Randomly select P_i Solve P_i
	$\xleftarrow{i}$	
(k_i)		(k_i)

12. Key Establishment

12.2 Key Distribution — Shamir's three-pass protocol

- In 1980, Adi Shamir proposed a key distribution protocol that employs commutative encryption

Table 12.2

Shamir's Three-Pass Protocol (error in the printed edition of the book)

A		B
(n)		(n)
$k \xleftarrow{r} \mathcal{K}$		
	$\xrightarrow{k_1 = E_{k_A}(k)}$	
	$\xleftarrow{k_2 = E_{k_B}(E_{k_A}(k))}$	
$D_{k_A}(k_2)$		
	$\xrightarrow{k_3 = E_{k_B}(k)}$	
		$D_{k_B}(k_3)$
(k)		(k)

12. Key Establishment

12.2 Key Distribution — Shamir's three-pass protocol

- An additive stream cipher, such as the one-time pad, yields a commutative encryption
- In this case, however, all encryptions cancel themselves out and the protocol gets totally insecure
- If r_A is the bit sequence used by A to compute k_1 and k_3, and r_B is the bit sequence used by B to compute k_2, then k_1, k_2, and k_3 can then be expressed as

$$\begin{aligned} k_1 &= r_A \oplus k \\ k_2 &= r_B \oplus k_1 = r_B \oplus r_A \oplus k \\ k_3 &= r_A \oplus k_2 = r_A \oplus r_B \oplus r_A \oplus k = r_B \oplus k \end{aligned}$$

12. Key Establishment

12.2 Key Distribution — Shamir's three-pass protocol

- These are the values an adversary can observe in a passive (wiretapping) attack
- The adversary can add k_1 and k_2 modulo 2 to retrieve r_B

$$k_1 \oplus k_2 \quad = \quad r_A \oplus k \oplus r_B \oplus r_A \oplus k = r_B$$

- This value can then be added modulo 2 to k_3 to determine k

$$r_B \oplus k_3 = r_B \oplus r_B \oplus k = k$$

12. Key Establishment

12.2 Key Distribution — Shamir's three-pass protocol

- The bottom line is that a perfectly secure symmetric encryption system is used, and yet the resulting key distribution protocol is totally insecure
- This suggests that the use of an additive stream cipher is inappropriate to instantiate the three-pass protocol
- Shamir suggested the use of modular exponentiation in $\mathbb{Z}_p^*$ (instead of an additive stream cipher)
- The resulting three-pass protocol is known as **Shamir's three-pass protocol** (or **Shamir's no key protocol**)

12. Key Establishment

12.2 Key Distribution — Shamir's three-pass protocol

- Respective values for k_1, k_2, and k_3:

$$\begin{aligned} k_1 &\equiv k^{e_A} \pmod{p} \\ k_2 &\equiv (k^{e_A})^{e_B} \equiv k^{e_A e_B} \pmod{p} \\ k_3 &\equiv ((k^{e_A})^{e_B})^{d_A} \\ &\equiv ((k^{e_A})^{d_A})^{e_B} \\ &\equiv (k^{e_A d_A})^{e_B} \\ &\equiv k^{e_B} \pmod{p} \end{aligned}$$

- B can use d_B to retrieve k:

$$k \equiv (k^{e_B})^{d_B} \equiv k^{e_B d_B} \equiv k \pmod{p}$$

12. Key Establishment

12.2 Key Distribution — Shamir's three-pass protocol

- In 1982, James L. Massey and Jim Omura proposed the use of a binary extension field $\mathbb{F}_{2^m}$ for $m \in \mathbb{N}$ (instead of $\mathbb{Z}_p^*$)
- The resulting variant of Shamir's three-pass protocol is known as the **Massey-Omura protocol**
- It allows hardware implementations to be more efficient
- All known instantiations of Shamir's three-pass protocol employ modular exponentiation in one way or another (and therefore refer to public key cryptography)

12. Key Establishment

12.2 Key Distribution — Asymmetric encryption-based key distribution protocol

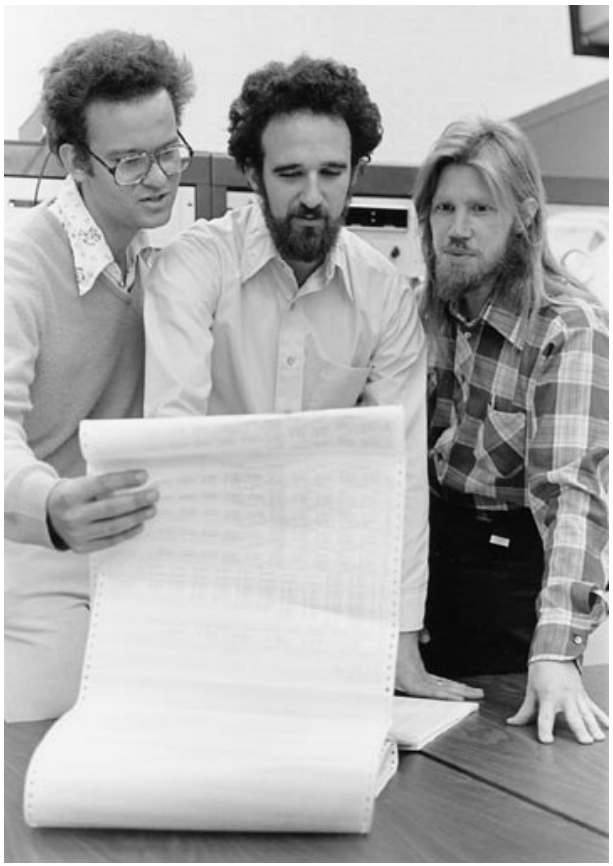
- Asymmetric encryption-based key distribution is used in many Internet security protocols (e.g., IPsec/IKE, SSL/TLS, . . .)

Table 12.3
An Asymmetric Encryption-based Key Distribution Protocol

A		B
(pk_B)		(sk_B)
$k \xleftarrow{r} \mathcal{K}$		
	$\xrightarrow{\text{Encrypt}(pk_B, k)}$	
		$k = \text{Decrypt}(sk_B, \text{Encrypt}(pk_B, k))$
(k)		(k)

12. Key Establishment

12.3 Key Agreement — Diffie-Hellman key exchange protocol



© 1977 Stanford News

- In 1976, Whitfield Diffie and Martin Hellman published a landmark paper entitled "New Directions in Cryptography"
- The paper introduced the notion of public key cryptography and proposed a key agreement protocol
- The paper changed the field
- Diffie and Hellman won the ACM A.M. Turing Award in 2015

12. Key Establishment

12.3 Key Agreement — Diffie-Hellman key exchange protocol

- The **Diffie-Hellman key exchange** (**exponential key exchange**) protocol can be used by two entities that have no prior relationship to agree on a secret key by communicating over a public but authentic channel
- As such, its existence seems paradoxical at first sight

Table 12.4
Diffie-Hellman Key Exchange

A		**B**
(G, g)		(G, g)
$x_a \xleftarrow{r} \mathbb{Z}_q^*$ $y_a = g^{x_a}$		$x_b \xleftarrow{r} \mathbb{Z}_q^*$ $y_b = g^{x_b}$
	$\xrightarrow{y_a}$	
	$\xleftarrow{y_b}$	
$k_{ab} = y_b^{x_a}$		$k_{ba} = y_a^{x_b}$
(k_{ab})		(k_{ba})

12. Key Establishment

12.3 Key Agreement — Diffie-Hellman key exchange protocol

- Toy example
  - $p = 23$ is a safe prime, because $11 = (23 - 1)/2$ is also prime
  - $\mathbb{Z}_{23}^* = \{1, \ldots, 22\}$ has a subgroup G that consists of the $q = 11$ elements 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, and 18
  - $g = 3$ is a generator of this group (there are others)
  - A randomly selects $x_a = 6$, computes $y_a = 3^6 \mod 23 = 16$, and sends this value to B
  - B randomly selects $x_b = 9$, computes $y_b = 3^9 \mod 23 = 18$, and sends this value to A
  - A computes $y_b^{x_a} = 18^6 \mod 23 = 8$
  - B computes $y_a^{x_b} = 16^9 \mod 23 = 8$
  - The result is $k = k_{ab} = k_{ba} = 8$

12. Key Establishment

12.2 Key Distribution — Diffie-Hellman key exchange protocol

Table 12.5
A MITM Attack Against the Diffie-Hellman Key Exchange Protocol

A	**C**	**B**
(G, g)		(G, g)
$x_a \xleftarrow{r} \mathbb{Z}_q^*$		$x_b \xleftarrow{r} \mathbb{Z}_q^*$
$y_a = g^{x_a}$		$y_b = g^{x_b}$
	$y_a \rightsquigarrow y_c$	
	$y_c \rightsquigarrow y_b$	
$k_{ac} = y_c^{x_a}$		$k_{bc} = y_c^{x_b}$
(k_{ac})		(k_{bc})

12. Key Establishment

12.3 Key Agreement — Diffie-Hellman key exchange protocol

- The source of the problem (i.e., susceptibility to MITM attack) is the lack of authenticity
- People therefore prefer an **authenticated Diffie-Hellman key exchange**, such as provided by the station-to-station (STS) protocol
- There are many possibilities to authenticate a Diffie-Hellman key exchange using complementary cryptographic techniques, such as passwords, secret keys, or digital signatures and public key certificates
- In the case of a password, the **encrypted key exchange (EKE)** protocol yields an alternative

12. Key Establishment

12.2 Key Distribution — Diffie-Hellman key exchange protocol

Table 12.7
ECDH Protocol

A		B
$(Curve, G, n)$		$(Curve, G, n)$
$d_a \xleftarrow{r} \mathbb{Z}_n \setminus \{0\}$		$d_b \xleftarrow{r} \mathbb{Z}_n \setminus \{0\}$
$Q_a = d_a G$		$Q_b = d_b G$
	$\xrightarrow{Q_a}$	
	$\xleftarrow{Q_b}$	
$k_{ab} = d_a Q_b$		$k_{ba} = d_b Q_a$
(k_{ab})		(k_{ba})

12. Key Establishment

12.2 Key Distribution — Diffie-Hellman key exchange protocol

- Toy example
  - $(Curve, G, n)$ from Chapter 5, i.e., $a = b = 1$ $(y^2 \equiv x^3 + x + 1)$, $p = 23$ $(\mathbb{Z}_{23})$, $G = (3, 10)$, and $n = 28$
  - A selects $d_a = 6$, computes $Q_a = 6G = 6(3, 10) = (12, 4)$, and sends $Q_a = (12, 4)$ to B
  - B selects $d_b = 11$, computes $Q_b = 11G = 11(3, 10) = (18, 20)$, and sends $Q_b = (18, 20)$ to A
  - A computes $d_a Q_b = 6(18, 20) = (6, 4)$
  - B computes $d_b Q_a = 11(12, 4) = (6, 4)$
  - Note that $6 \cdot 11(3, 10) = 11 \cdot 6(3, 10) = 66 \bmod 28(3, 10) \equiv 10(3, 10) = (6, 4)$

12. Key Establishment

12.4 Quantum Cryptography

- **Quantum cryptography** refers to a key establishment technology that is based on the laws of quantum physics (instead of mathematics)
- More specifically, it makes use of the **Heisenberg uncertainty principle**
- This principle states that certain pairs of physical quantities of an object, such as its position and velocity, cannot both be measured exactly at the same time
- This has practical implications for the exceedingly small masses of atoms and subatomic particles, like photons

12. Key Establishment

12.4 Quantum Cryptography

- To measure the polarization of a photon, one can use one of two bases:
  - A **rectilinear basis** (⊞) is able to reliably distinguish between photons that are polarized horizontally with 0°/180° (↔) or vertically with 90°/270° (↕)
  - A **diagonal basis** (⊠) is able to reliably distinguish between photons that are polarized diagonally, i.e., with either 45°/225° (⤢) or 135°/315° (⤡)
- The two bases (i.e., ⊞ and ⊠) are **conjugate** in the sense that the measurement of the polarization in one basis randomizes the measurement in the other basis
- This can be exploited to establish a **quantum channel**

12. Key Establishment

12.4 Quantum Cryptography

- In 1984, Charles H. Bennett and Gilles Brassard proposed a quantum cryptography-based key exchange protocol known as **quantum key exchange (QKE)**
- A may send out photons in one of four polarizations: $\leftrightarrow$, $\nearrow$, $\updownarrow$, or $\nwarrow$
- B measures the polarizations of the photons it receives
- According to the laws of quantum physics, B can distinguish between rectilinear polarizations (i.e., $\leftrightarrow$ or $\updownarrow$ using $\boxplus$) and diagonal polarizations (i.e., $\nearrow$ or $\nwarrow$ using $\boxtimes$), but it cannot distinguish between both types of polarization simultaneously

12. Key Establishment

12.4 Quantum Cryptography

- Coding rules (encoding and decoding)
  - Rectilinear basis (⊞)
    - Horizontal polarization with 0°/180° (↔) stands for 0
    - Vertical polarization with 90°/270° (↕) stands for 1
  - Diagonal basis (⊠)
    - Diagonal polarization with 45°/225° (⤢) stands for 0
    - Diagonal polarization with 135°/315° (⤡) stands for 1

12. Key Establishment

12.4 Quantum Cryptography

Table 12.8
An Exemplary Transcript of the Quantum Key Exchange Protocol

1)	0	0	1	0	1	1	0	1	1	0
2)	⊞	⊠	⊠	⊞	⊠	⊞	⊞	⊠	⊠	⊞
3)	↔	⤢	⤡	↔	⤡	↕	↔	⤡	⤡	↔
4)	⊞	⊞	⊠	⊞	⊞	⊠	⊞	⊞	⊠	⊠
5)	0		1	0	*0*	*0*	0	*1*	1	*0*
6)	⊞		⊠	⊞	⊞	⊠	⊞	⊞	⊠	⊠
7)	✓		✓	✓			✓		✓	
8)	0		1	0			0		1	
9)			1				0			
10)			✓				✓			
11)	0			0					1	

12. Key Establishment

12.4 Quantum Cryptography

- Advantages
  - Provides an alternative key exchange method (whose security does not depend on mathematics)
  - Resistant to quantum computing
- Disadvantages (problem areas)
  - Requires specialized hardware (costs)
  - Requires and authentic channel (bootstrap problem)
  - Relatively small distances ($\approx$ 100 km)
  - Must be combined with "conventional" cryptography
  - ...

12. Key Establishment

12.4 Quantum Cryptography

- Many researchers have contributed to quantum cryptography in many ways
- In 1991, Artur Ekert proposed an alternative QKE protocol that uses entangled photons
- In addition to quantum key distribution protocols (using polarized or entangled photons), many other quantum cryptographic protocols have been developed and proposed
- A few companies sell quantum cryptographic devices and products, such as ID Quantique and MagiQ Technologies

12. Key Establishment

12.5 Final Remarks

- The Diffie-Hellman key exchange protocol is omnipresent (i.e., it is used in almost all Internet security protocols)
- Whenever two entities want to establish a secret key, it provides an elegant and highly efficient solution
- Using bilinear maps, it can be generalized to three entities
- The generalization to > 3 entities remains an open problem
- People use Diffie-Hellman trees to come up with key exchange protocols that have a complexity that grows "only" logarithmically with the number of entities (e.g., IETF MLS WG)

Questions and Answers

Thank you for your attention