Hans Delfs & Helmut Knebl:

Kryptographie und Informationssicherheit

WS 2008/2009


References

Lehrbuch zur Vorlesung


Weitere Lehrbuecher:


The fundamental and classical task of cryptography is to provide confidentiality by encryption methods. The message to be transmitted – it can be some text, numerical data, an executable program or any other kind of information – is called the plaintext. Alice encrypts the plaintext \( m \) and obtains the ciphertext \( c \). The ciphertext \( c \) is transmitted to Bob. Bob turns the ciphertext back into the plaintext by decryption. To decrypt, Bob needs some secret information, a secret decryption key.

Every encryption method provides an encryption algorithm \( E \) and a decryption algorithm \( D \). In classical encryption schemes, both algorithms depend on the same secret key \( k \). This key \( k \) is used for both encryption and decryption. These encryption methods are therefore called symmetric. For example, in Caesar’s cipher the secret key is the offset 3 of the shift. We have

\[
D(k, E(k, m)) = m \text{ for each plaintext } m.
\]

In 1976, W. Diffie and M.E. Hellman published their famous paper, New Directions in Cryptography. There they introduced the revolutionary concept of public-key cryptography. They provided a solution to the long standing problem of key exchange and pointed the way to digital signatures. The public-key encryption methods are asymmetric. Each recipient of messages has his personal key \( k = (pk, sk) \), consisting of two parts: \( pk \) is the encryption key and is made public, \( sk \) is the decryption key and is kept secret. If Alice wants to send a message \( m \) to Bob, she encrypts \( m \) by use of Bob’s publicly known encryption key \( pk \). Bob decrypts the ciphertext by use of his decryption key \( sk \), which is known only to him. We have

\[
D(sk, E(pk, m)) = m.
\]

Providing confidentiality is not the only objective of cryptography. Cryptography is also used to provide solutions for other problems:

1. Data integrity.
2. Authentication.
There are symmetric as well as public-key methods to ensure the integrity of messages. Classical symmetric methods require a secret key $k$ that is shared by sender and receiver. The message $m$ is augmented by a message authentication code (MAC). The code is generated by an algorithm and depends on the secret key. The augmented message $(m, MAC(k, m))$ is protected against modifications. The receiver may test the integrity of an incoming message $(m, \bar{m})$ by checking whether $MAC(k, m) = \bar{m}$.

Message authentication codes may be implemented by keyed hash functions.

Digital signatures require public-key methods. As with classical handwritten signatures, they are intended to provide authentication and non-repudiation. If Alice wants to sign the message $m$, she applies the algorithm $Sign$ with her secret key $sk$ and gets the signature $Sign(sk, m)$. Bob receives a signature $s$ for message $m$, and may then check the signature by testing whether $Verify(pk, s, m) = ok$, with Alice’s public key $pk$.

**Definition 1.** A symmetric-key encryption scheme consists of a map $E : K \times M \rightarrow C$, such that for each $k \in K$, the map $E_k : M \rightarrow C, m \mapsto E(k, m)$ is invertible. The inverse function $D_k := E_k^{-1}$ is called the decryption function. It is assumed that efficient algorithms to compute $E_k$ and $D_k$ exist.

The key $k$ is shared between the communication partners and kept secret. A basic security requirement for the encryption map $E$ is that without knowing the key $k$, it should be impossible to successfully execute the decryption function $D_k$. Important examples of symmetric-key encryption schemes – Vernam’s one-time pad, DES and AES – are given below.
**Stream Ciphers**

**Definition 2.** Let $K$ be a set of keys and $M$ be a set of plaintexts. In this context, the elements of $M$ are called characters.

A stream cipher

$$E^*: K^* \times M^* \rightarrow C^*, E^*(k, m) := c := c_1c_2c_3\ldots$$

encrypts a stream $m := m_1m_2m_3\ldots \in M^*$ of plaintext characters $m_i \in M$ as a stream $c := c_1c_2c_3\ldots \in C^*$ of ciphertext characters $c_i \in C$ by using a *key stream* $k := k_1k_2k_3\ldots \in K^*, k_i \in K$.

The plaintext stream $m = m_1m_2m_3\ldots$ is encrypted character by character.

**For this purpose, there is an encryption map**

$$E: K \times M \rightarrow C,$$

which encrypts the single plaintext characters $m_i$ with the corresponding key character $k_i$:

$$c_i = E_{k_i}(m_i) = E(k_i, m_i), i = 1, 2, \ldots$$

Typically, the characters in $M$ and $C$ and the key elements in $K$ are binary digits or bytes.

**Block Ciphers**

**Definition 3.** A *block cipher* is a symmetric-key encryption scheme with $M = C = \{0, 1\}^n$ and key space $K = \{0, 1\}^r$:

$$E: \{0, 1\}^r \times \{0, 1\}^n \rightarrow \{0, 1\}^n.$$

Using a secret key $k$ of binary length $r$, the encryption algorithm $E$ encrypts plaintext blocks of a fixed binary length $n$ and the resulting ciphertext blocks also have length $n$. $n$ is called the *block length* of the cipher.

Typical block lengths are 64 (as in DES) or 128 (as in AES), typical key lengths are 56 (as in DES) or 128, 192 and 256 (as in AES).
**Electronic Codebook Mode**

In this mode, we have \( r = n \). The electronic codebook mode is implemented by the following algorithm:

**Algorithm 6.**

\[
\text{bitString } ecbEncrypt(\text{bitString } m) \\
1 \text{ divide } m \text{ into } m_1 \ldots m_l \\
2 \text{ for } i \leftarrow 1 \text{ to } l \text{ do} \\
3 \quad c_i \leftarrow E_k(m_i). \\
4 \text{ return } c_1 \ldots c_l
\]

For decryption, the same algorithm can be used with the decryption function \( E_k^{-1} \) in place of \( E_k \).

**Cipher-Block Chaining Mode**

In this mode, we have \( r = n \). Encryption in the cipher-block chaining mode is implemented by the following algorithm:

**Algorithm 7.**

\[
\text{bitString } cbcEncrypt(\text{bitString } m) \\
1 \text{ select } c_0 \in \{0, 1\}^n \text{ at random} \\
2 \text{ divide } m \text{ into } m_1 \ldots m_l \\
3 \text{ for } i \leftarrow 1 \text{ to } l \text{ do} \\
4 \quad c_i \leftarrow E_k(m_i \oplus c_{i-1}) \\
5 \text{ return } c_0c_1 \ldots c_l
\]

**The Euclidean Algorithm.**

Let \( a, b \in \mathbb{Z}, a > b > 0 \). The greatest common divisor \( \gcd(a, b) \) can be computed by an iterated division with remainder. Let \( r_0 := a, r_1 := b \) and

\[
\begin{align*}
    r_0 &= q_1 r_1 + r_2, & 0 < r_2 < r_1, \\
    r_1 &= q_2 r_2 + r_3, & 0 < r_3 < r_2, \\
    &\vdots \\
    r_{k-1} &= q_k r_k + r_{k+1}, & 0 < r_{k+1} < r_k, \\
    &\vdots \\
    r_{n-2} &= q_{n-1} r_{n-1} + r_n, & 0 < r_n < r_{n-1}, \\
    r_{n-1} &= q_n r_n + r_{n+1}, & 0 = r_{n+1}.
\end{align*}
\]

By construction, \( r_1 > r_2 > \ldots \). Therefore, the remainder becomes 0 after a finite number of steps. The last remainder \( \neq 0 \) is the greatest common divisor, as is shown in the next proposition.
The Binary Encoding of Numbers.

The sequence $z_{k-1}z_{k-2}\ldots z_1z_0$ of bits $z_i \in \{0, 1\}, 0 \leq i \leq k - 1$, is the encoding of $n = z_0 + z_1 \cdot 2^1 + \ldots + z_{k-2} \cdot 2^{k-2} + z_{k-1} \cdot 2^{k-1} = \sum_{i=0}^{k-1} z_i \cdot 2^i$.

In public-key cryptography, we usually have to compute with remainders modulo $n$. This means that the computations take place in the residue class ring $\mathbb{Z}_n$.

**Definition 15.** Let $n \in \mathbb{N}, n \geq 2$:
1. $a, b \in \mathbb{Z}$ are congruent modulo $n$, written as $a \equiv b \mod n$, if $n$ divides $a - b$. This means that $a$ and $b$ have the same remainder when divided by $n$: $a \mod n = b \mod n$.
2. Let $a \in \mathbb{Z}$. $[a] := \{x \in \mathbb{Z} \mid x \equiv a \mod n\}$ is called the residue class of $a$ modulo $m$.
3. $\mathbb{Z}_n := \{[a] \mid a \in \mathbb{Z}\}$ is the set of residue classes modulo $n$.

**Definition 16.** By defining addition and multiplication as $[a] + [b] = [a + b]$ and $[a] \cdot [b] = [a \cdot b]$, $\mathbb{Z}_n$ becomes a commutative ring, with unit element $[1]$. It is called the residue class ring modulo $n$.

**Definition 17.** Let $R$ be a commutative ring with unit element $e$. An element $x \in R$ is called a unit if there is an element $y \in R$ with $x \cdot y = e$. We call $y$ a multiplicative inverse of $x$. The subset of units is denoted by $R^*$.

**Remark.** The multiplicative inverse of a unit $x$ is uniquely determined, and we denote it by $x^{-1}$. The set of units $R^*$ is a subgroup of $R$ with respect to multiplication.
Proposition 18. An element \([x] \in \mathbb{Z}_n\) is a unit if and only if \(\gcd(x, n) = 1\). The multiplicative inverse \([x]^{-1}\) of a unit \([x]\) can be computed using the extended Euclidean algorithm.

Corollary 19. Let \(p\) be a prime. Then every \([x] \neq [0]\) in \(\mathbb{Z}_p\) is a unit. Thus, \(\mathbb{Z}_p\) is a field.

Definition 20. The subgroup
\[\mathbb{Z}_n^* := \{x \in \mathbb{Z}_n \mid x \text{ is a unit in } \mathbb{Z}_n\}\]
of units in \(\mathbb{Z}_n\) is called the prime residue class group modulo \(n\).

Definition 21. Let \(M\) be a finite set. The number of elements in \(M\) is called the cardinality or order of \(M\). It is denoted by \(|M|\).

We introduce the Euler phi function, which gives the number of units modulo \(n\).

Definition 22. \[\varphi : \mathbb{N} \rightarrow \mathbb{N}, \ n \mapsto |\mathbb{Z}_n^*|\]
is called the Euler phi function or the Euler totient function.
Proposition 23 (Euler).

\[ \sum_{d \mid n} \varphi(d) = n. \]

Corollary 24. Let \( p \) be a prime and \( k \in \mathbb{N} \). Then \( \varphi(p^k) = p^k - (p - 1) \).

Proof. By Euler’s result, \( \varphi(1) + \varphi(p) + \ldots + \varphi(p^k) = p^k \) and \( \varphi(1) + \varphi(p) + \ldots + \varphi(p^{k-1}) = p^{k-1} \). Subtracting both equations yields \( \varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p - 1) \). \( \square \)

Proposition 25. Let \( G \) be a finite group and \( e \) be the unit element of \( G \). Then \( x^{[G]} = e \) for all \( x \in G \).

Proposition 26 (Fermat). Let \( p \) be a prime and \( a \in \mathbb{Z} \) be a number that is prime to \( p \) (i.e. \( p \) does not divide \( a \)). Then

\[ a^{p-1} \equiv 1 \mod p. \]

Proposition 27 (Euler). Let \( n \in \mathbb{N} \) and let \( a \in \mathbb{Z} \) be a number that is prime to \( n \). Then

\[ a^{\varphi(n)} \equiv 1 \mod n. \]

Definition 33. Let \( G \) be a finite group and let \( e \) be the unit element of \( G \). Let \( x \in G \). The smallest \( n \in \mathbb{N} \) with \( x^n = e \) is called the order of \( x \). We write this as \( \text{ord}(x) \).