Mathematics for Applied Cryptography I and II

Joel Häberli

March 7, 2023

Contents

1 Intent of the document

Collect mathematics and mathematical explanations for the modules *Applied Cryptography I and II* in one place.

2 Execution time of symmetric and public-key schemes

Symmetric schemes are remarkably faster than public-key schemes. Additionally the difference of execution time doesn't grow linearly if compared. This means that public-key schemes are growing slower in terms of execution time than symmetric schemes (While RSA with 1024 Bit keys was 10 times slower than AES, the difference of RSA with 3072 Bit keys and AES is bigger by a factor $x > 1$). One could state that given the functions

$$\begin{aligned} ts(n) &= \text{time of the symmetric scheme with key-length } n \text{ and} \\ tpk(n) &= \text{time of the public-key scheme with key-length } n \end{aligned}$$

the derivatives behave like:

$$\frac{\partial ts}{\partial n} > \frac{\partial tpk}{\partial n}$$

Which means that tpk grows slower than ts for a linearly growing length n.

3 Modular Arithmetic and Grouptheory

3.1 Primes

1. Prime counting function $\pi(n)$. Counts all primes in $\{1, .., n\}$.
   (a) Remember: Sieve of Eratosthenes
2. The prime theorem states, that approximately $\pi(n) = \frac{n}{\ln(n)}$ is valid.

3.2 Modular Arithmetic

1. The fundamental theorem of the modular arithmetik says, that *each natural number can be expressed as product of primes.* This leads to the prime factorization:
$$n = p_1^{e_1} p_2^{e_2} ... p_k^{e_k} = \Pi_{i=1}^{k} p_i^{e_i}$$
2. GCD (Greatest Common Divisor) $d = gcd(a, b)$ (de: ggT, grösster Gemeinsamer Teiler), for two numbers $a < b < n$ and a $d \in \{1, .., n\}$.
3. Eulers Totient Function $\phi(n)$ (In the course of discrete mathematics it was called Eulers Phi-Function). The function counts all numbers which are divider foreign to the argument n given as input of the function. This function defines numbers which are called *relatively prime to the group*

over the elements $\{1, .., n\}$: Over the given elements $\{1, .., n\}$ the numbers $\phi(n)$ possess the same properties as the primes over $\mathbb{Z}$. There exist some simplifications for certain decompositions of n given as:

(a) $\phi(n) = n \cdot \Pi_{i=1}^{k}(1 - \frac{1}{p_i})$, for n an arbitrary decomposition in primes.

(b) $\phi(p) = p - 1$, for p prim $(n = p)$.

(c) $\phi(pq) = (p - 1)(q - 1)$, for p, q prim $(n = p \cdot q)$.

3.3 Groups

1. Properties of a group G
   (a) *Associativity*
   (b) *Identity*
   (c) *Inverse*
   (d) A group is called *abelian* if also the *commutativity* is given. Be aware that this is special property and does not apply to all groups, but only abelian.
   (e) The *order* of a group is determined by the numbers of elements contained. This means each finite group has an order.
2. Additive Groups modulo n
3. Multiplicative Groups modulo n
4. Order of a group *element* (rem: not the same as order of the group!)
5. Generators
6. Cyclic Groups
7. Subgroups and Lagranges Theorem