ETH Zurich, Department of Computer Science
SS 2020

Prof. Ueli Maurer
Dr. Martin Hirt
Chen-Da Liu Zhang

Cryptographic Protocols
Notes 1

Scribe: Sandro Coretti (modified by Chen-Da Liu Zhang)

About the notes: These notes serve as written reference for the topics not covered by the papers that are handed out during the lecture. The material contained therein is thus a *strict* subset of what is relevant for the final exam.

These notes provide some basics for students not familiar with elementary number theory and algebra, a description of the RSA public-key encryption system, and some important facts about quadratic residues. Finally, the notes contain a short treatment of asymptotics and the concept of a distinguisher.

1.1 Groups

A *group* is a mathematical structure $\langle G; * \rangle$ consisting of a non-empty set G and a binary operation $* : G \times G \to G$ and satisfying the following axioms:

(A1) The operation $*$ is *associative*, i.e., for any $x, y, z \in G$, $x * (y * z) = (x * y) * z$.

(A2) There exists a *neutral element* e for $*$, i.e., $x * e = e * x = x$ for all $x \in G$.

(A3) Every element $x \in G$ has an inverse $\hat{x}$, i.e., $x * \hat{x} = \hat{x} * x = e$.

If $*$ is commutative, then G is called an *abelian* or *commutative* group. Often, $*$ is denoted by $+$, inverses by $-$, and the neutral element by 0, in which case one speaks of an *additive* group. Similarly, if the above are denoted by $\cdot$, $^{-1}$, and 1, respectively, one speaks of a *multiplicative* group.

Simple examples of groups are the integers with addition, i.e., $\langle \mathbb{Z}; + \rangle$, the reals without zero and with multiplication, i.e., $\langle \mathbb{R} \setminus \{0\}; \cdot \rangle$, or the integers $0, \ldots, n-1$ with addition modulo n, i.e., $\langle \mathbb{Z}_n, \oplus_n \rangle$.

The *order* $|G|$ *of* G is the number of elements in G. The *order* $\mathrm{ord}(x)$ *of* $x \in G$ is the least natural number k such that $x^k := \underbrace{x * \ldots * x}_{k \text{ times}} = e$.[1] An important theorem states that $\mathrm{ord}(x)$ divides $|G|$ for every $x \in G$. Consequently, $x^{|G|} = e$.

Consider a finite group G. G is *cyclic* if there exists an element $g \in G$, called *generator*, such that $G = \{g^0, g^1, \ldots, g^{p-1}\}$. In such a case, one says that g *generates* G, which is denoted by $G = \langle g \rangle$.

[1] In particular, $\mathrm{ord}(e) = 1$.

Two groups $\langle G; * \rangle$ and $\langle H : \star \rangle$ are called *isomorphic*, denoted by $G \cong H$, if there exists a bijection $\psi : G \to H$, called an *isomorphism*, such that for all $x, y \in G$

$$\psi(x * y) = \psi(x) \star \psi(y).$$

Intuitively, this means that the groups G and H are "the same" up to relabeling the elements.[2] An example of isomorphic groups is given in Section 1.4.

1.2 Inverses Modulo m and the Group $\mathbb{Z}_m^*$

Two numbers $x, y \in \mathbb{Z}$ are said to be *congruent modulo* m, denoted by

$$x \equiv y \pmod{m},$$

if m divides $(x - y)$. A number y is an *inverse modulo* m *of* x if

$$x \cdot y \equiv 1 \pmod{m}.$$

If x and m are coprime, x has an inverse modulo m, and the *extended Euclidean algorithm (EEA)* can be used to find an inverse modulo m of x, since computing the greatest common divisor of x and m with the EEA yields numbers $u, v \in \mathbb{Z}$ such that

$$ux + vm = \gcd(x, m) = 1,$$

which implies that $xu \equiv 1 \pmod{m}$, i.e., u is an inverse modulo m of x. Inverses y, y' modulo m of x are congruent modulo m, i.e., $y \equiv y' \pmod{m}$, as the reader can easily verify.

The above implies that $\langle \mathbb{Z}_m^*; \odot_m \rangle$, where $\mathbb{Z}_m^* := \{x \in \mathbb{Z} \mid 0 \leq x < m, \gcd(x, m) = 1\}$ and where $\odot_m$ is multiplication modulo m, is a group (the neutral element is 1).

If $m = pq$ for two primes p and q, then $|\mathbb{Z}_m^*| = (p - 1)(q - 1)$.[3]

1.3 The RSA Scheme

Pubic key encryption (PKE) schemes allow an entity Bob to create a key pair, consisting of a public and a secret key, such that every entity Alice in possession of Bob's public key may encrypt messages such that only Bob, who has the secret key, can decrypt them.

In the RSA scheme, Bob generates a key pair as follows: He chooses two large random primes p and q and computes $m := pq$. Moreover, he chooses a (not necessarily random) e such that $\gcd(e, f) = 1$ for $f := |\mathbb{Z}_m^*| = (p - 1)(q - 1)$. The latter implies that e has an inverse d modulo f and that therefore $ed = kf + 1$ for some $k \in \mathbb{Z}$. Bob publishes (n, e) as the public key and keeps d (which he computes using the EEA) as the secret key.

Alice encrypts a message $x \in \mathbb{Z}_m^*$ by computing the ciphertext $c := x^e$ (in $\mathbb{Z}_m^*$). When Bob obtains c, he computes

$$c^d = x^{ed} = x^{kf+1} = (x^f)^k \cdot x = x,$$

since $x^f = 1$ in $\mathbb{Z}_m^*$.

In order for the RSA system to be secure, it must necessarily be hard to factor m, as an attacker who knows p and q can easily compute the secret key d from these values. Note, however, that the hardness of factoring is only known to imply the hardness of breaking RSA in *restricted models of computation* (which is the relevant direction if the security of RSA is to be based on factoring). Moreover, RSA as presented is *deterministic*, which is not sufficient for most applications, and therefore needs to be randomized appropriately.

[2] Note that in general it may be difficult to efficiently compute group isomorphisms ψ.

[3] There is also a formula for general m, which is not discussed here.

1.4 The Chinese Remainder Theorem

Consider a system of r congruence relations

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ &\vdots \qquad\qquad \vdots \\ x &\equiv a_r \pmod{m_r}, \end{aligned}$$

where $m_1, \ldots, m_r$ are pairwise disjoint moduli. In such a case, the Chinese Remainder Theorem (CRT) states that there exists a *unique solution* x with $0 \leq x < M := \prod_i m_i$.

To find the solution, let $M_i := M/m_i$ for $i = 1, \ldots, r$. Then, for all i, $\gcd(M_i, m_i) = 1$ and $M_j \equiv 0 \pmod{m_i}$ for $j \neq i$. The former implies that M_i has an inverse N_i modulo m_i. That is,

$$M_i N_i \equiv 1 \pmod{m_i}$$

and thus

$$a_i M_i N_i \equiv a_i \pmod{m_i},$$

while still

$$a_j M_j N_j \equiv 0 \pmod{m_i},$$

for $j \neq i$. Thus,

$$R_M \left(\sum_{i=1}^{r} a_i M_i N_i \right)$$

satisfies all relations above, where $R_n(x)$ denotes the (unique) remainder when dividing x by n. The reader can prove the uniqueness of the above solution as an exercise.

An important consequence of the CRT is that for $m = pq$, $\langle \mathbb{Z}_m^*; \odot_m \rangle$ is isomorphic to $\langle \mathbb{Z}_p^* \times \mathbb{Z}_q^*; \odot_{p,q} \rangle$, where $\odot_{p,q}$ is the component-wise multiplication modulo p resp. q, via the isomorphism

$$\psi : \mathbb{Z}_m^* \to \mathbb{Z}_p^* \times \mathbb{Z}_p^*, \quad x \mapsto (R_p(x), R_q(x)),$$

which the reader should verify.[4] Put simply, instead of computing on integers modulo m, one can compute on pairs of integers modulo p on the first component and modulo q on the second.

1.5 Quadratic Residues

Let $m \in \mathbb{N} \setminus \{0\}$. A (integer) number a is called a *quadratic residue modulo* m if there exists a (integer) number r, called a *square root modulo* m *of* a, such that

$$r^2 \equiv a \pmod{m}.$$

Otherwise, a is a *quadratic non-residue*.

For a prime p, one defines the Legendre symbol

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p, \\ 0 & \text{if } a \text{ is divisible by } p, \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p. \end{cases}$$

[4] This means showing that ψ satisfies the isomorphism property above and that it is a bijection; the latter can be shown using the CRT.

Multiplying two quadratic residues or two quadratic non-residues results in a quadratic residue. Multiplying a quadratic residue and a quadratic non-residue results in a quadratic non-residue. In other words, the Legendre symbol satisfies

$$\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right).$$

One can show that in $\mathbb{Z}_p^*$, which has order $|\mathbb{Z}_p^*| = p-1$, there are exactly $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic non-residues. That is, a number a either has two square roots r and r', which are in fact related by $r \equiv -r' \pmod{p}$, or none.

Euler proved that

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}},$$

which is known as *Euler's criterion*. The reader may look up a proof of it on the internet as an exercise.

Consider now $m = pq$ for two primes p and q, and let $a \in \mathbb{Z}_m^*$. Recall the isomorphism ψ between $\mathbb{Z}_m^*$ and $\mathbb{Z}_p^* \times \mathbb{Z}_q^*$ from above. The isomorphism property implies that

$$r^2 = a \iff \psi(r^2) = \psi(a) \iff (R_p(r^2), R_q(r^2)) = (R_p(a), R_q(a)).$$

That is, r is a square root of a in $\mathbb{Z}_m^*$ if and only if $R_p(r)$ is a square root of $R_p(a)$ in $\mathbb{Z}_p^*$ and $R_q(r)$ is a square root of $R_q(a)$ in $\mathbb{Z}_q^*$. Since a number in $\mathbb{Z}_p^*$ resp. $\mathbb{Z}_q^*$ has two or no square roots, every number in $\mathbb{Z}_m^*$ has either four square roots or none.

1.6 Polynomial, Negligible, and Noticeable Functions

A function $f : \mathbb{N} \to \mathbb{R}^+$ is *polynomial* if it can be upper bounded by some polynomial, i.e., if

$$\exists c \in \mathbb{N} : \exists n_0 : \forall n \geq n_0 : f(n) \leq n^c.$$

An algorithm is called *efficient* if its running time grows polynomially in the input length.

A function $f : \mathbb{N} \to \mathbb{R}^+$ is *negligible* if it decreases (to 0) faster than the inverse of every polynomial, i.e., if

$$\forall c \in \mathbb{N} : \exists n_0 : \forall n \geq n_0 : f(n) \leq \frac{1}{n^c}.$$

A function $f : \mathbb{N} \to \mathbb{R}^+$ is *noticeable* if it can be lower bounded by the inverse of some polynomial, i.e., if

$$\exists c \in \mathbb{N} : \exists n_0 : \forall n \geq n_0 : f(n) \geq \frac{1}{n^c}.$$

Note that noticeable is not the negation of negligible.

In general, one can also consider other efficiency and negligibility notions, provided they satisfy certain natural conditions. For example, if an efficient algorithm with negligible probability of breaking a scheme is repeated "efficiently" many times, it should still have negligible probability of doing so. The reader may check that the above standard notions satisfy this.