Institute of Computer Science, University of Bern
Cryptography, HS 2019

Prof. Christian Cachin
Luca Zanolini

Exercise 9

9.1 Diffie-Hellman assumptions (4 pts)

Let $\mathbb{G}$ be a cyclic group of order q, such that g is a generator of $\mathbb{G}$ and such that the Discrete Logarithm Problem and related problems are hard.

Recall the *Decisional Diffie-Hellman (DDH)* assumption, which states that

$\mathcal{L}^{\mathbb{G}}_{\text{dh-real}}$	$\approx$	$\mathcal{L}^{\mathbb{G}}_{\text{dh-rand}}$
QUERY():		QUERY():
$a, b \leftarrow \mathbb{Z}_q$		$a, b, c \leftarrow \mathbb{Z}_q$
return (g^a, g^b, g^{ab})		return (g^a, g^b, g^c)

In other words, any polynomial-time algorithm cannot distinguish between g^{ab} and g^c with non negligible probability.

A related assumption is the *Computational Diffie-Hellman (CDH)* assumption, which states that given g^a, g^b, an attacker cannot compute g^{ab} in polynomial time with non-negligible probability.

a) Describe the Computational Diffie-Hellman assumption with two indistinguishable libraries. *Hint:* Recall the *Bad-Event Lemma* and the corresponding discussion from Sec. 4.3 in [R19].

b) What is the relation between these two assumptions? What happens if one can break the CDH assumption?

9.2 Man-in-the-middle attack (3 pts)

Assume Alice and Bob want to use Diffie-Hellman key exchange to generate a shared secret key, which they can use for encryption. Let $\mathbb{G}$ be a public common cyclic group of order n and g a generator of $\mathbb{G}$. Alice picks $a \leftarrow \mathbb{Z}_n$ and Bob chooses $b \leftarrow \mathbb{Z}_n$. Alice sends g^a to Bob and Bob sends g^b to Alice. Assume Eve, a (wo)man in the middle, who is able to intercept both g^a and g^b and modify them in a way that Bob receives $g^{a'}$ and Alice receives $g^{b'}$.

What is the resulting public key K for Alice? And for Bob? What can Eve do?

9.3 Quadratic residues (3 pts)

A number $x \in \mathbb{Z}_n^*$ is a *quadratic residue modulo* n if there exists some y such that $y^2 \equiv_n x$, i.e., if x can be obtained by squaring a number mod n.

Let p be an odd prime and let $\mathbb{QR}_p^* = \{x \in \mathbb{Z}_p^* \mid \exists y : x \equiv_p y^2\}$. For this case, one can easily find out for any $x \in \mathbb{Z}_p^*$ whether $x \in \mathbb{QR}_p^*$ by checking whether

$$x^{\frac{p-1}{2}} \stackrel{?}{\equiv}_p 1.$$

If $x^{\frac{p-1}{2}} \equiv_p 1$, then $x \in \mathbb{QR}_p^*$, and otherwise $x \notin \mathbb{QR}_p^*$. This follows from *Euler's criterion*, for which one can find proofs online. Note that the test leaks one bit about the discrete logarithm of x. This criterion is a reason for not using the multiplicative group $\mathbb{Z}_p^*$ itself as the basis for cryptosystems relying on the decisional Diffie-Hellman assumption.

However, it is easy to find a quadratic residue of $\mathbb{Z}_p^*$ using the following result: Show that if g is a primitive root of $\mathbb{Z}_p^*$, then $< g^2 >= \mathbb{QR}_p^*$. In particular, this means that $g^a \in \mathbb{QR}_p^*$ if and only if a is even – and the choice of generator g does not matter.