Introduction to Cryptography

TEK 4500 (Fall 2020)

Problem Set 8

Problem 1.

Read Chapter 9 (Section 9.4 can be skipped) and Chapter 10.1–10.2 in [BR].

Problem 2.

Let $G_3 = \{e, a, b\}$ and $G_4 = \{e, a, b, c\}$. Decide whether $(G_3, \diamond)$, $(G_3, \trianglerighteq)$, $(G_4, \circledcirc)$, $(G_4, \oslash)$, $(G_4, \boxdot)$ are groups, where $\diamond$, $\trianglerighteq$, $\circledcirc$, $\oslash$, $\boxdot$ are the binary operations defined by the following multiplication tables.

$\diamond$	e	a	b
e	e	a	b
a	b	e	e
b	a	b	a

$\trianglerighteq$	e	a	b
e	b	e	a
a	e	a	b
b	a	b	e

$\circledcirc$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	c	b	a	e
c	b	c	e	a

$\oslash$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

$\boxdot$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Problem 3.

a) List all elements of $\mathbf{Z}_{17}$.

b) List all elements of $\mathbf{Z}_{17}^*$.

c) Find a generator for $(\mathbf{Z}_{17}, +)$ different from 1.

d) Find a generator for $(\mathbf{Z}_{17}^*, \cdot)$.

e) List all subgroups of $(\mathbf{Z}_{17}, +)$.

f) List all subgroups of $(\mathbf{Z}_{17}^*, \cdot)$.

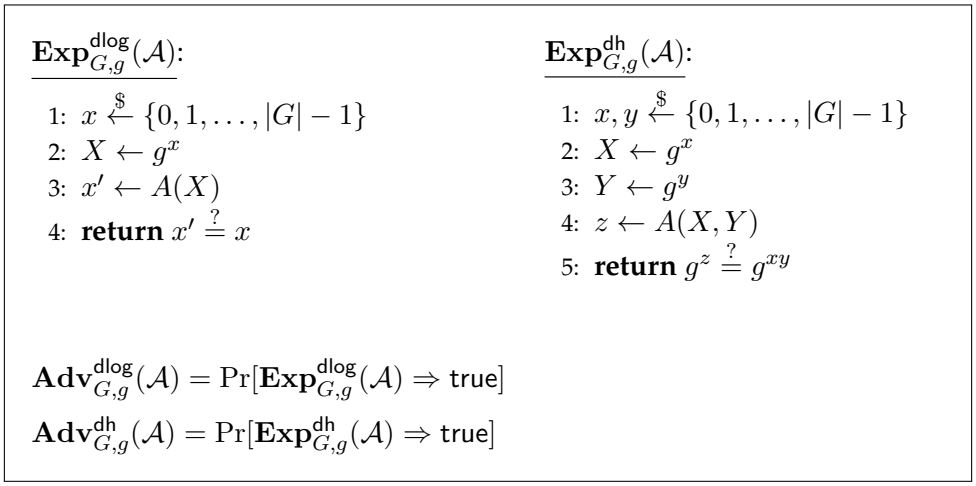

Figure 1: Formal security experiments for the discrete logarithm (DLOG) problem and the Diffie-Hellman problem in a cyclic group $G = \langle g \rangle$.

Problem 4.

In this exercise we'll see why $(\mathbf{Z}_n, +)$—the additive group of integers modulo n—is not a good choice for Diffie-Hellman. Specifically, we'll see that the discrete logarithm problem (DLOG) is very easy to solve in $(\mathbf{Z}_n, +)$ (thus, as we saw in the lecture, the Diffie-Hellman problem is also easy to solve).

a) Specialize the DLOG experiment $\mathbf{Exp}^{\mathsf{dlog}}_{G,g}(\mathcal{A})$ in Fig. 1 to the case of $G = (\mathbf{Z}_n, +)$. That is, define what set x is drawn from at Line 1 and how X is created at Line 2 for the specific case of $G = (\mathbf{Z}_n, +)$. You may assume that the generator is $g = 1$ if you want.

b) Define a DLOG adversary $\mathcal{A}$ against $(\mathbf{Z}_n, +)$ having $\mathbf{Adv}^{\mathsf{dlog}}_{(\mathbf{Z}_n,+),1}(\mathcal{A}) = 1$.

c) Suppose $n = 124908349700012358124024534503482350534539534500924 21$ and you're given $X = 712037902312771231671940120948148711182471298712947 9 \in \mathbf{Z}_n$. What's the discrete logarithm of X in $(\mathbf{Z}_n, +)$ assuming $g = 1$?

d) What's the discrete logarithm of X if $g = 7$?

Hint: X is not a prime number (which you can verify here).

Problem 5.

Given the prime $p = 541$, let $G = (\mathbf{Z}_p^*, \cdot)$.

$\mathbf{Exp}^{\mathsf{dlog}}_{(\mathbf{Z}_n,+),1}(\mathcal{A})$:

1: $x \xleftarrow{\$} \{0, 1, \ldots, |\mathbf{Z}_n| - 1\}$
2: $X \leftarrow x \cdot 1 \pmod{n}$
3: $x' \leftarrow A(X)$
4: **return** $x' \stackrel{?}{=} x$

$\mathbf{Adv}^{\mathsf{dlog}}_{(\mathbf{Z}_n,+),1}(\mathcal{A}) = \Pr[\mathbf{Exp}^{\mathsf{dlog}}_{(\mathbf{Z}_n,+),1}(\mathcal{A}) \Rightarrow \mathsf{true}]$

Figure 2: DLOG security experiment specialized to the group $(\mathbf{Z}_n, +) = \langle 1 \rangle$.

a) What are the possible orders that the subgroups of G can have?

b) Is G a good choice to use for the Diffie-Hellman key exchange protocol?

Problem 6.

Given the prime $p = 402947$. Alice and Bob use the group $(\mathbf{Z}_p^*, \cdot)$ for the Diffie-Hellman key exchange protocol. They use 2 as the generator for $(\mathbf{Z}_p^*, \cdot)$.

a) Verify that 2 is a generator for $(\mathbf{Z}_p^*, \cdot)$. You can either write a program that verifies this, or you can use the theory in Section 9.3[1] of [BR] to prove it yourself (hint: p is a safe prime).

b) Suppose $A = 2^a = 97592$ is the value sent from Alice to Bob, and that $B = 2^b = 112792$ is the value sent from Bob to Alice. Implement the baby-step, giant-step algorithm in a programming language of your choice, and use it to find the key $Z = 2^{ab} \pmod{p}$ shared by Alice and Bob.

Hint: The inverse of 2 in $(\mathbf{Z}_p^*, \cdot)$ is $2^{-1} = 201474 \pmod{p}$

Problem 7.

Prove formally that DH security (according to the right-hand side of Fig. 1) implies DLOG security (according to the left-hand side of Fig. 1).

Hint: Prove the equivalent contrapositive statement: DLOG insecurity implies DH insecurity. That is, suppose you had an algorithm $\mathcal{A}$ that could solve the DLOG problem. Show how you could use $\mathcal{A}$ to create an algorithm $\mathcal{B}$ that solves the DH problem. What's the DH-advantage of $\mathcal{B}$, i.e., what's $\mathbf{Adv}^{\mathsf{dh}}_{G,g}(\mathcal{B})$?

[1] In particular, look at Proposition 9.13. Example 9.15 is also useful.

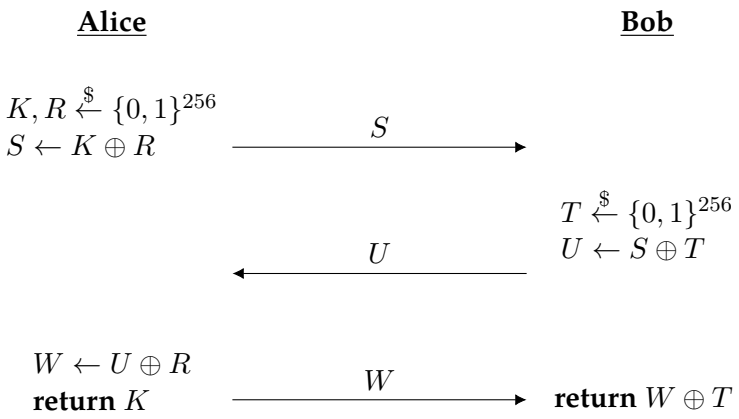

Figure 3: A key-exchange proposal.

Problem 8. [Problem 9.3 in [KL07]]
Consider the key-exchange protocol shown in Fig. 3. Show that Alice and Bob output the same key. Analyze the security of the scheme (i.e., either argue why an adversary can't obtain the shared key or show a concrete attack).

References

[BR] Mihir Bellare and Phillip Rogaway. *Introduction to Modern Cryptography*. https://web.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf.

[KL07] Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography*. Chapman and Hall/CRC Press, 2007.