CISC 468: CRYPTOGRAPHY

LESSON 11: DIFFIE-HELLMAN KEY EXCHANGE

Furkan Alaca

READINGS

- Section 8.1: Diffie-Hellman Key Exchange, Paar & Pelzl
- Section 8.2: Some Algebra, Paar & Pelzl
- Section 8.3: The Discrete Logarithm Problem, Paar & Pelzl
- Section 8.4: Security of the Diffie-Hellman Key Exchange, Paar & Pelzl

ONE-WAY FUNCTIONS

- The computational infeasibility of reversing the RSA encryption function is based on the difficulty of the *integer factorization problem*
- Other asymmetric algorithms rely on different problems that are difficult to solve
- We will see two asymmetric algorithms that rely on the *discrete logarithm problem*:
  - Diffie-Hellman Key Exchange
  - Elgamal Encryption Scheme

DIFFIE-HELLMAN KEY EXCHANGE

- The Diffie-Hellman Key Exchange (DHKE) was the first asymmetric scheme to be published, in 1976
- DHKE enables two communicating parties to agree on a secret key over an insecure channel
  - Secure against *passive attacks*, but insufficient on its own to defend against *active attacks*
  - The secret key is then typically used for symmetric encryption, e.g., with AES

DHKE: WHY IT WORKS

- Exponentiation with sufficiently large exponents in $\mathbb{Z}_p^*$, where p is prime, is:
  - A one-way function: Given $\alpha^x = \beta \bmod p$, it is computationally infeasible to recover x
  - Commutative: $(\alpha^x)^y = (\alpha^y)^x \bmod p$

DHKE: SET-UP

- A set-up protocol (executed by either communicating party, or by a trusted third-party) is required prior to the key exchange:

1. Choose a large prime p.
2. Choose an integer $\alpha \in \{2, 3, \ldots, p-2\}$.
3. Publish p and α.

- The values p and α are referred to as *domain parameters* and are publicly-known.
- p should have similar length as the RSA modulus n (i.e., 2048 bits) and α is required to have a special property

DHKE: MAIN PROTOCOL

1. Alice selects a private key $a \in \{2, 3, \ldots, p-2\}$, computes $A \equiv \alpha^a \mod p$, and sends A to Bob.
2. Bob selects a private key $b \in \{2, 3, \ldots, p-2\}$, computes $B \equiv \alpha^b \mod p$, and sends A to Alice.
3. Alice computes $k_{AB} = B^a \equiv (\alpha^b)^a \mod p$.
4. Bob computes $k_{AB} = A^b \equiv (\alpha^a)^b \mod p$.
5. Alice and Bob initiate secure communication using k_{AB}, e.g., as a symmetric key for encryption.

For properly-chosen parameters p and α, it is computationally infeasible for a passive attacker to compute k_{AB}, given A and B.

DHKE: EXAMPLE

Assume the domain parameters are $p = 29$ and $\alpha = 2$:

1. Alice chooses $a = 5$, computes $A = 2^5 \equiv 3 \mod 29$, and sends A to Bob.
2. Bob chooses $b = 12$, computes $B = 2^{12} \equiv 7 \mod 29$, and sends B to Alice.
3. Alice computes $k_{AB} = B^a = 7^5 \equiv 16 \mod 29$.
4. Bob computes $k_{AB} = A^b = 3^{12} \equiv 16 \mod 29$.

Note that we chose small values here for illustrative purposes, but these are insecure (i.e., not one-way) for real-world use!

DHKE: IMPLEMENTATION CONSIDERATIONS

- Alice and Bob's private exponents a and b need to be chosen using a true random number generator, in order to prevent attackers from guessing them
- The computation that needs to be done, i.e., exponentiation, is similar to that of RSA—both parties can make use of the square-and-multiply algorithm

GROUP THEORY REVIEW: DEFINITION

A group is a set G together with an operation $\star$ that has the following properties:

1. Closed on $\star$: For all $a, b \in G, a \star b = c \in G$.
2. Associative on $\star$: That is, $a \star (b \star c) = (a \star b) \star c$.
3. Identity element: There exists $1 \in G$ such that $a \star 1 = 1 \star a = a$ for all $a \in G$.
4. For each $a \in G$ there is an inverse $a^{-1} \in G$ where $a \star a^{-1} = a^{-1} \star a = 1$.

The group is called abelian if it is commutative, i.e., $a \star b = b \star a$ for all $a, b \in G$.

GROUP THEORY REVIEW: ORDER OF AN ELEMENT

- Theorem: $\mathbb{Z}_n^*$, consisting of $i = 1, 2, \ldots, n-1$ for which $\gcd(i, n) = 1$, forms an abelian group under multiplication modulo n. The identity element is $e = 1$.
- Definition: The order $\mathrm{ord}(a)$ of an element a of a group $(G, \star)$ is the smallest positive integer k such that

$$a^k = \underbrace{a \star a \star \cdots \star a}_{k \text{ times}} = 1,$$

where 1 is the identity element of G.

GROUP THEORY REVIEW: EXAMPLE 1

Example: We determine the order of $a = 3$ in the group $\mathbb{Z}_{11}^*$:

$$
\begin{aligned}
a^1 &= 3 \\
a^2 &= 3 \cdot 3 = 9 \\
a^3 &= 9 \cdot 3 = 27 \equiv 5 \bmod 11 \\
a^4 &= 5 \cdot 3 = 15 \equiv 4 \bmod 11 \\
a^5 &= 4 \cdot 3 = 12 \equiv 1 \bmod 11
\end{aligned}
$$

From the last line, it follows that $\mathrm{ord}(3) = 5$.

GROUP THEORY REVIEW: EXAMPLE 1 (CONT'D)

Continuing the example, we keep multiplying the result by a:

$$
\begin{aligned}
a^6 &= a^5 \cdot a = 1 \cdot 3 \equiv 3 \bmod 11 \\
a^7 &= a^5 \cdot a^2 = 1 \cdot 9 \equiv 9 \bmod 11 \\
a^8 &= a^5 \cdot a^3 = 1 \cdot 5 \equiv 5 \bmod 11 \\
a^9 &= a^5 \cdot a^4 = 1 \cdot 4 \equiv 4 \bmod 11 \\
a^{10} &= a^5 \cdot a^5 = 1 \cdot 1 \equiv 1 \bmod 11 \\
a^{11} &= a^{10} \cdot a = 1 \cdot 3 \equiv 3 \bmod 11 \\
&\vdots
\end{aligned}
$$

The resulting sequence repeats $\{3, 9, 5, 4, 1\}$ indefinitely

GROUP THEORY REVIEW: CYCLIC GROUPS

- A group G that contains an element α with maximum order $\text{ord}(\alpha) = |G|$ is said to be *cyclic*
- Elements with maximum order are called *primitive elements* or *generators*

GROUP THEORY REVIEW: EXAMPLE 2

Consider the group $\mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. So, $|\mathbb{Z}_{11}^*| = 10$. We want to check if $a = 2$ is a primitive element of the group:

$$
\begin{aligned}
a^1 &\equiv 2 \bmod 11 & a^6 &\equiv 9 \bmod 11 \\
a^2 &\equiv 4 \bmod 11 & a^7 &\equiv 7 \bmod 11 \\
a^3 &\equiv 8 \bmod 11 & a^8 &\equiv 3 \bmod 11 \\
a^4 &\equiv 5 \bmod 11 & a^9 &\equiv 6 \bmod 11 \\
a^5 &\equiv 10 \bmod 11 & a^{10} &\equiv 1 \bmod 11
\end{aligned}
$$

It follows from the last result that $\text{ord}(a) = 10 = |\mathbb{Z}_{11}^*|$. This implies that $a = 2$ is a primitive element and $\mathbb{Z}_{11}^*$ is cyclic.

THE DISCRETE-LOGARITHM PROBLEM (DLP)

Given the finite cyclic group $\mathbb{Z}_p^*$ of order $p-1$, a primitive element $\alpha \in \mathbb{Z}_p^*$ and another element $\beta \in \mathbb{Z}_p^*$, the DLP is the problem of determining the integer $1 \leq x \leq p-1$ such that:

$$\alpha^x = \beta \bmod p.$$

- The integer $x = \log_\alpha \beta \bmod p$ is called the *discrete logarithm* of β to the base α.
  - Always exists, since α is a primitive element
  - Very hard to compute if parameters are sufficiently large

DLP: EXAMPLE

Consider a discrete logarithm in the group $\mathbb{Z}_{47}^*$, in which $\alpha = 5$ is a primitive element. For $\beta = 41$, the discrete logarithm problem is to find the integer x such that

$$5^x \equiv 41 \mod 47.$$

By systematically trying all possible values for x, we obtain the solution $x = 15$.

DLP: GROUP CARDINALITY

- In practice, defense against known mathematical attacks requires us to use groups with prime cardinality,
- $\mathbb{Z}_p^*$ has cardinality $p - 1$, which is composite
- But subgroups of $\mathbb{Z}_p^*$ with prime cardinality exist, so we can use those instead of $\mathbb{Z}_p^*$ itself

DLP: USING A SUBGROUP WITH PRIME CARDINALITY

Consider the group $\mathbb{Z}_{47}^*$ which has cardinality 46. Its subgroups thus have cardinalities of 23, 2, and 1. Note that 23 is prime and $\alpha = 2$ is a primitive element in the subgroup with 23 elements.

A possible discrete logarithm problem is given for $\beta = 36$ (also in the subgroup): Find the integer x such that

$$2^x = 36 \bmod 47.$$

By an exhaustive search, we obtain the solution $x = 17$.

GENERALIZED DLP

The DLP can be generalized to cyclic groups aside from just the multiplicative group $\mathbb{Z}_p^*$.

Given a finite cyclic group G with the group operation $\circ$ and cardinality n, we consider a primitive element $\alpha \in G$ and another element $\beta \in G$. The generalized discrete logarithm problem is finding the integer x, where $1 \leq x \leq n$, such that

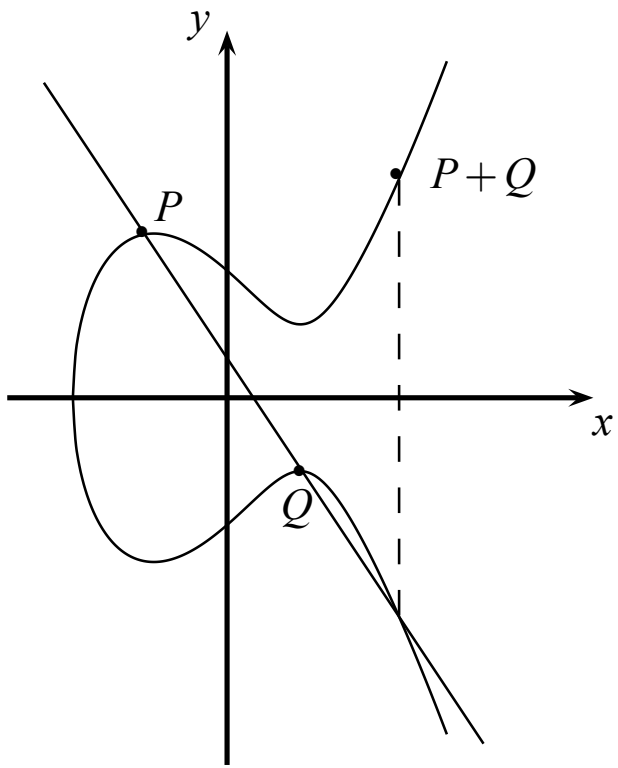
$$\beta = \underbrace{\alpha \circ \alpha \circ \cdots \circ \alpha}_{x \text{ times}} = \alpha^x.$$

GENERALIZED DLP

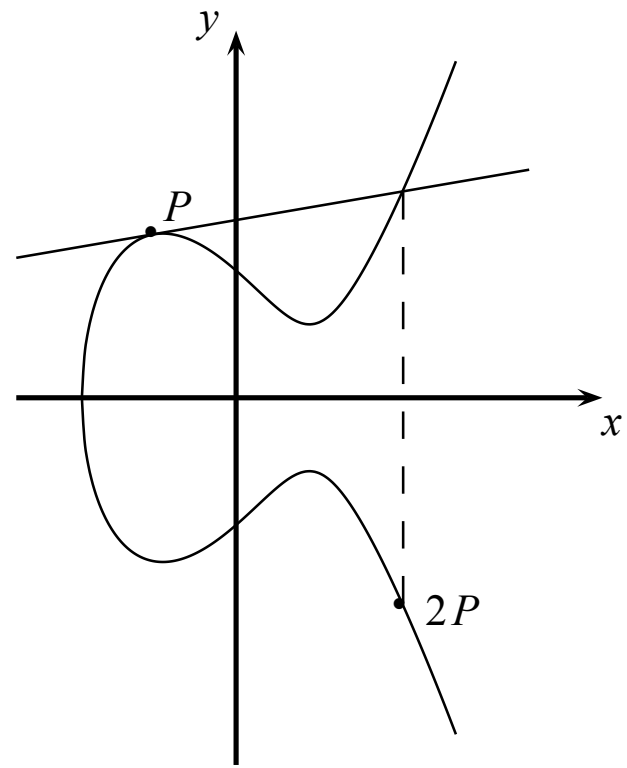
- There are cyclic groups in which the DLP is not difficult, and such groups cannot be used for a public-key cryptosystem
- The multiplicative group of the prime field $\mathbb{Z}_p$, or a subgroup of it, is used by the classical DHKE as well as Elgamal encryption and the Digital Signature Algorithm (DSA)
- DHKE can also use the cyclic group formed by points on an elliptic curve
  - This has become more popular over the last decade

EXTRA: ELLIPTIC CURVES

$y^2 = x^3 - 3x + 3$ over $\mathbb{R}$



Point addition on an elliptic curve over the real numbers



Point doubling on an elliptic curve over the real numbers