Discrete Logarithms

Schedule for today

Recap

Discrete Logarithms & Key Agreement
The DLOG problem
Key Agreement
DH Key Agreement

Security of Diffie Hellman
The DDH problems and relation to DLOG
Passive Security of DHKA
MITM attacks on DH
Generalizing DH & Elliptic Curve Groups

What we did last time

Questions

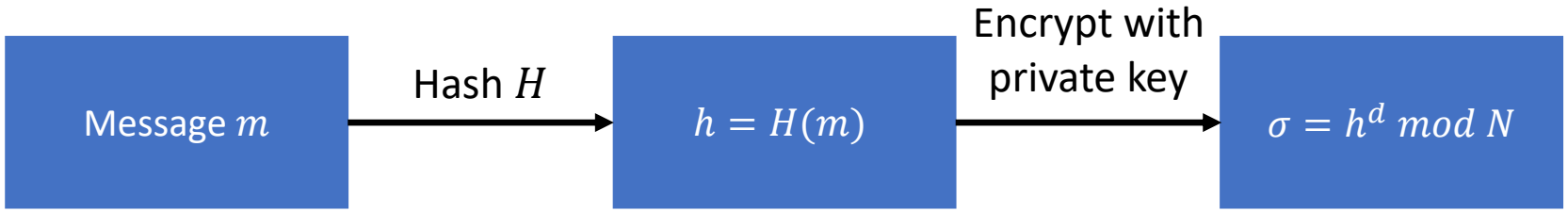
The RSA-FDH signature scheme allows multiple signatures for the same message.

Digital Signatures using RSA: RSA-FDH

Signing key: secret d

Verification key N, e

Cryptographic hash $H: \{0,1\}^* \rightarrow Z_N^*$



Verify m, σ:

Check that $H(m) = \sigma^e \ mod \ N$

Any RSA instance for encryption can also be used for signing!

Questions

There exist prime numbers p for which the Fermat test falsely claims that they are not prime.

Questions

The Miller-Rabin test only probabilistically determines if a number is prime (i.e. with high probability the output is correct).

Discrete Logarithms & Key Agreement

Order of a group element

Let p be a prime and $g \in Z_p^*$.

Then the smallest positive $a \in N$ such that $g^a = 1 \; mod \; p$ is called *order of* g mod p.

E.g. $p = 31$.

Element	1	2	3	4
Order $mod \; p$	1	5	30	5

Lagrange's Theorem

For any finite group G and subgroup $H \subseteq G$: $|\mathrm{H}|$ divides $|G|$.

Corollary:
For any prime p and $g \in Z_p^*$ the order of g must divide $\phi(p) = p - 1$

Fact:

For any prime p there are $\phi(\phi(p))$ many elements $g \in Z_p^*$ that have maximal order $\phi(p) = p - 1$.

Finding elements of maximal order

Easy mode:
Let p be a prime such that $p - 1 = 2q$ where q is also prime.

1. Pick $g \in Z_p^*$ such that $g \notin \{1, p-1\}$
2. If $g^q \neq 1 \bmod p$ then output g, otherwise go to step 1

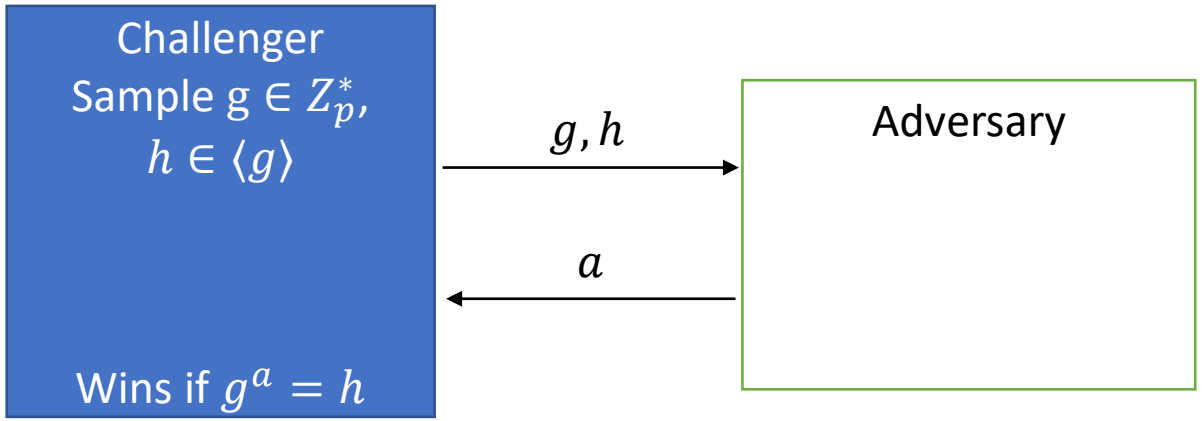
General:

Let p be any prime.

1. Pick $g \in Z_p^*$.
2. For every q that divides $p - 1$ test that $g^q \neq 1 \bmod p$. If so then output g, otherwise go to step 1

Discrete logarithms modulo a prime

Let p be a prime



Discrete logarithms modulo a prime

Example

$$p = 17, g = 3, h = 14$$

a	1	2	3	4	5	6	7	8	9
$3^a \ mod \ 17$	3	9	10	13	5	15	11	16	14

Hardness of DLOG

When is DLOG difficult?

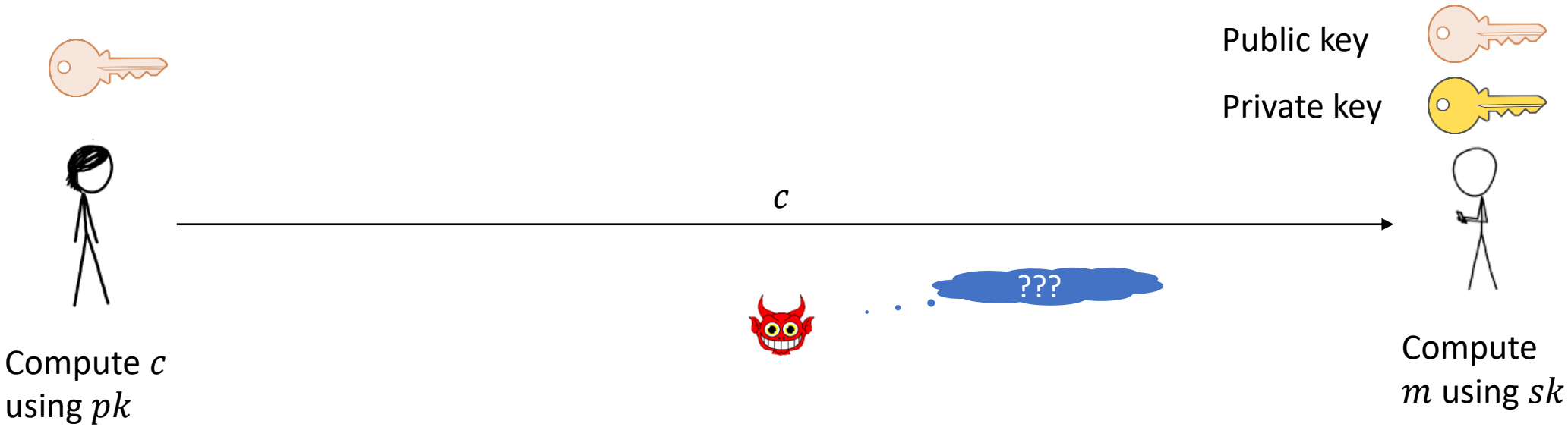
1. p is large prime (brute force attacks)
2. $p - 1$ must have at least one large prime factor (exercise!)
3. q must be large (brute force attacks)

Difficulty until 2030:

Keylength.com: use $\log_2 p \approx 15.000$

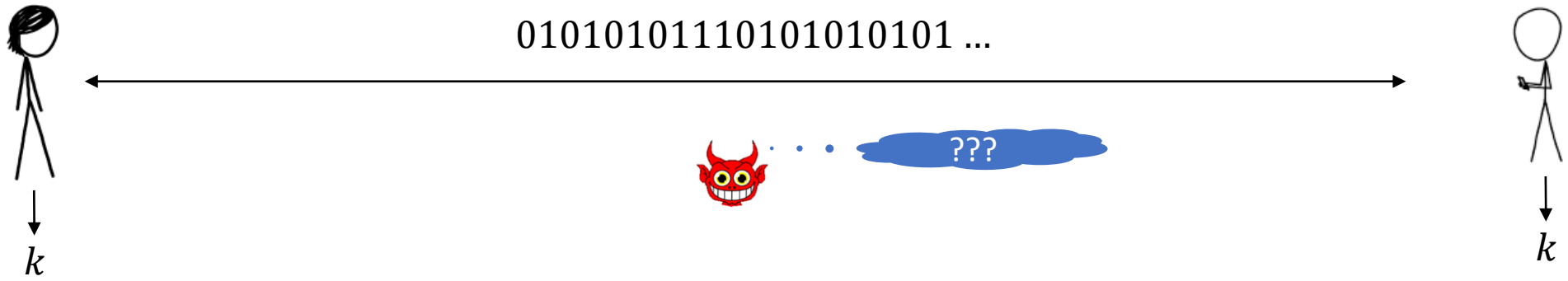
What does DLOG have to do with Cryptography?

So far: Public key encryption



What if Alice does not know any public key of Bob??

The key-agreement problem

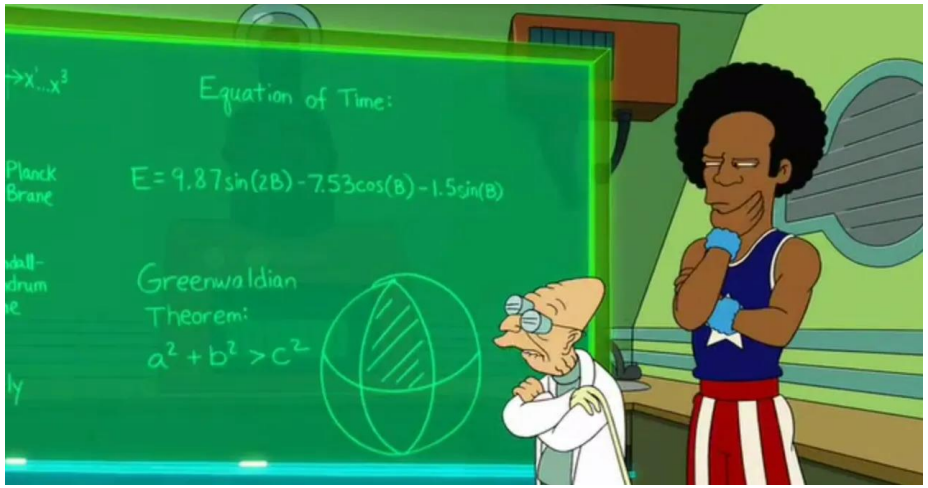


Alice has no special secret information about Bob and vise-versa

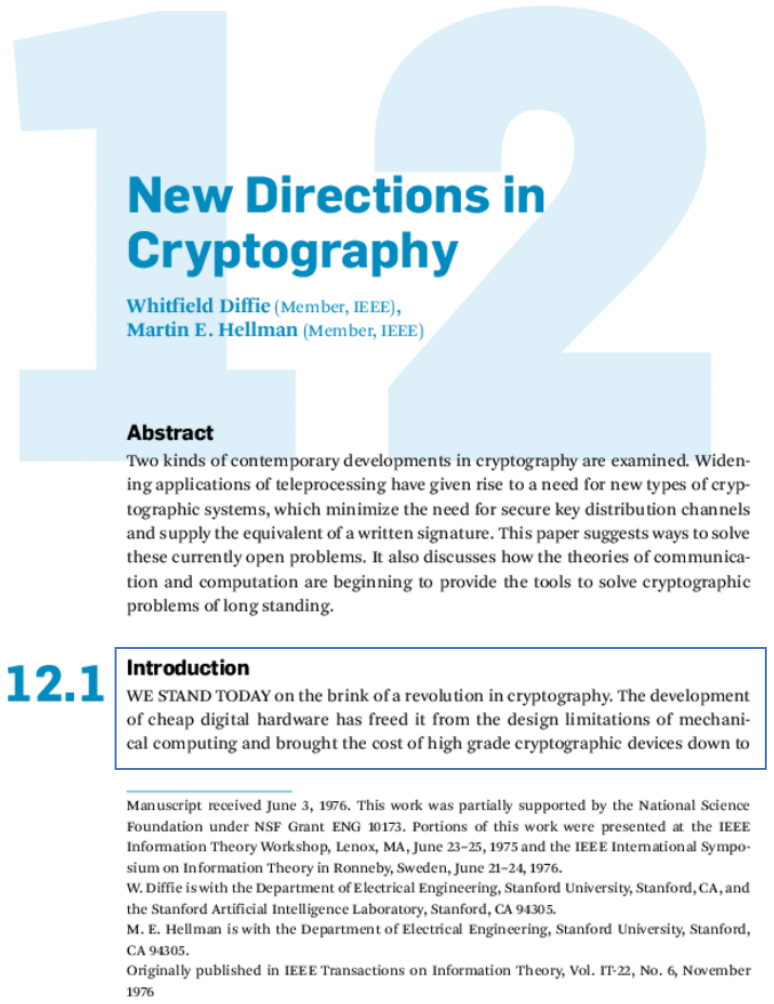
The key-agreement problem

Seems impossible:
how to agree on something private over public channel?

Solution:
Discrete Logarithms!



1976: Diffie and Hellman have an idea…



12

New Directions in Cryptography

Whitfield Diffie (Member, IEEE),
Martin E. Hellman (Member, IEEE)

Abstract

Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems of long standing.

12.1 Introduction

WE STAND TODAY on the brink of a revolution in cryptography. The development of cheap digital hardware has freed it from the design limitations of mechanical computing and brought the cost of high grade cryptographic devices down to

Manuscript received June 3, 1976. This work was partially supported by the National Science Foundation under NSF Grant ENG 10173. Portions of this work were presented at the IEEE Information Theory Workshop, Lenox, MA, June 23–25, 1975 and the IEEE International Symposium on Information Theory in Ronneby, Sweden, June 21–24, 1976.

W. Diffie is with the Department of Electrical Engineering, Stanford University, Stanford, CA, and the Stanford Artificial Intelligence Laboratory, Stanford, CA 94305.
M. E. Hellman is with the Department of Electrical Engineering, Stanford University, Stanford, CA 94305.

Originally published in IEEE Transactions on Information Theory, Vol. IT-22, No. 6, November 1976

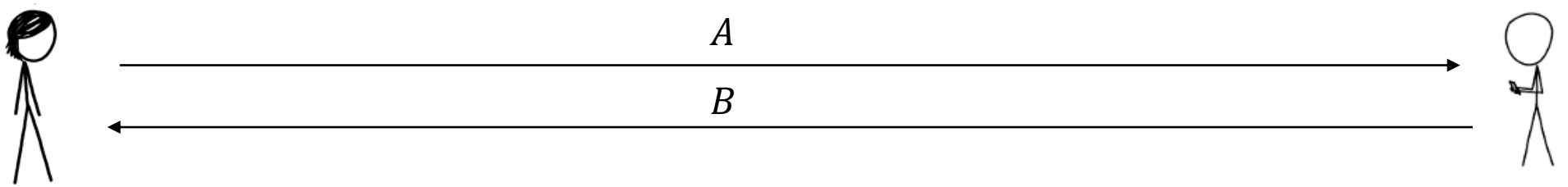
Turing Award in 2015

Diffie Hellman key agreement

Fix large primes p, q where $q|p-1$

Fix $g \in Z_p^*$ such that g has order q

Public information!



1. Choose random $a \in Z_q$
2. Compute $A = g^a \ mod \ p$
3. Output $k = B^a \ mod \ p$

1. Choose random $b \in Z_q$
2. Compute $B = g^b \ mod \ p$
3. Output $k = A^b \ mod \ p$

Diffie Hellman key agreement

Why it works

$$B^a = \left(g^b\right)^a = g^{ab} = (g^a)^b = A^b$$

Example

$p = 23, g = 5$

Alices chooses $a = 4$, Bob chooses $b = 7$

Exchanged messages: $A = 4, B = 17$

$17^4 = 4^7 = 8\ mod\ 23$

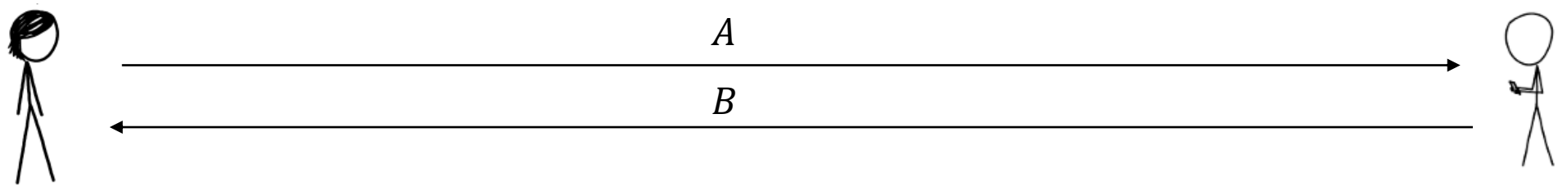
Security of Diffie Hellman

Security of Diffie Hellman

Fix large primes p, q where $q|p-1$

Fix $g \in Z_p^*$ such that g has order q

Public information!



1. Choose $\in Z_q$
2. Comput $mod\ p$
3. Output $od\ p$

Attacker's task:
Given g, A, B find k

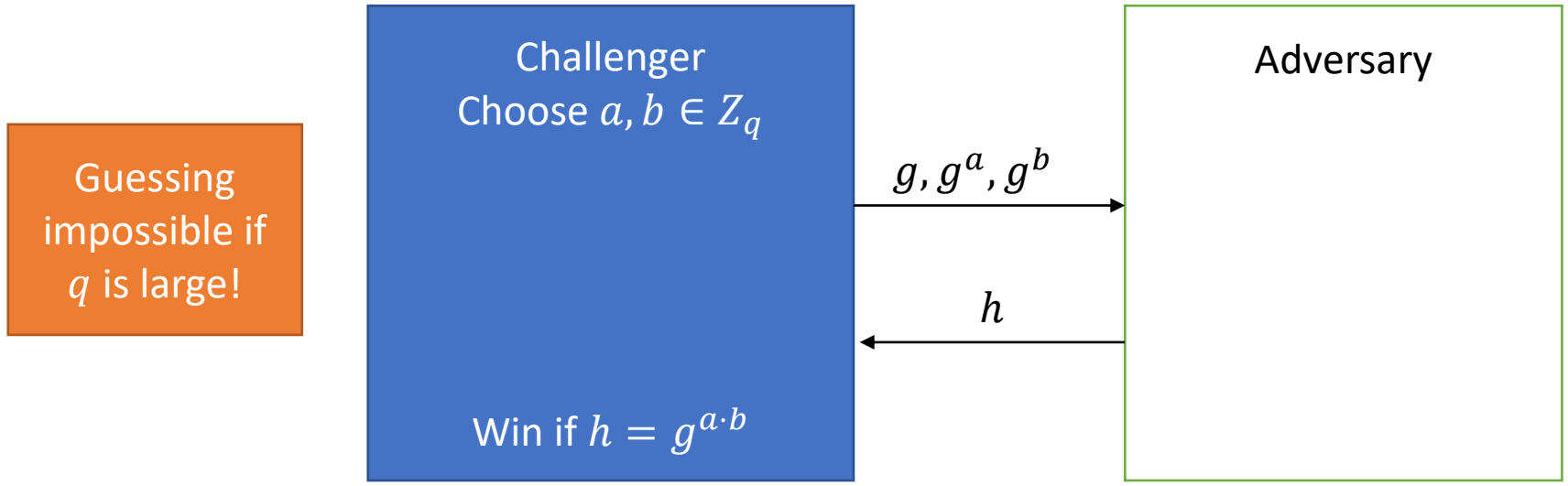
Clearly, DLOG must be difficult!

But breaking DH is not the same as DLOG…

Computational Diffie Hellman Problem (CDH)

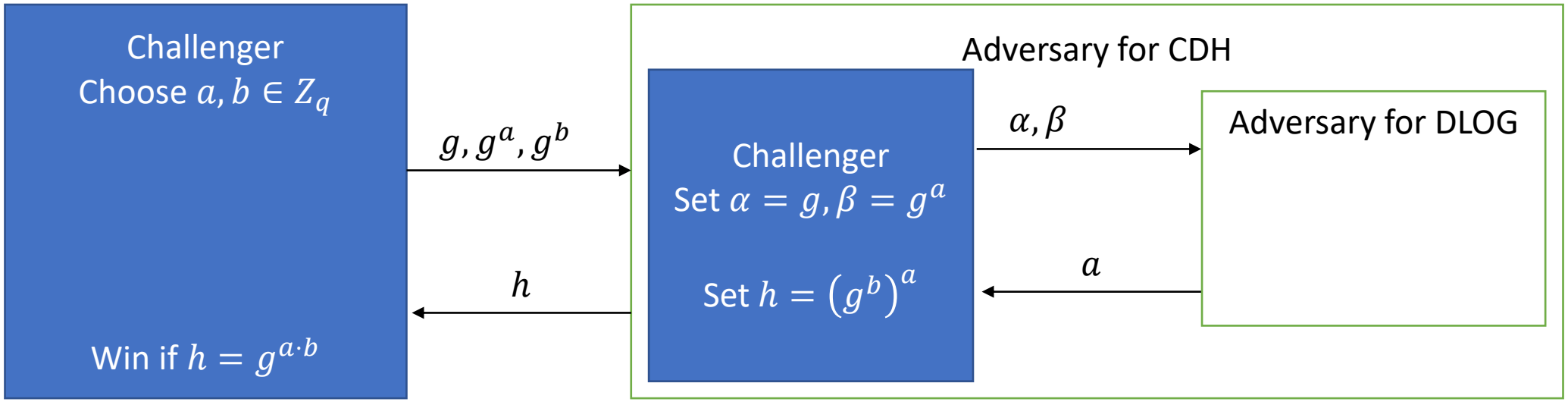
Fix large primes p, q where $q|p-1$

Fix $g \in Z_p^*$ such that g has order q



CDH vs. DLOG

Attack on DLOG => Attack on CDH



Reverse is not known in general!

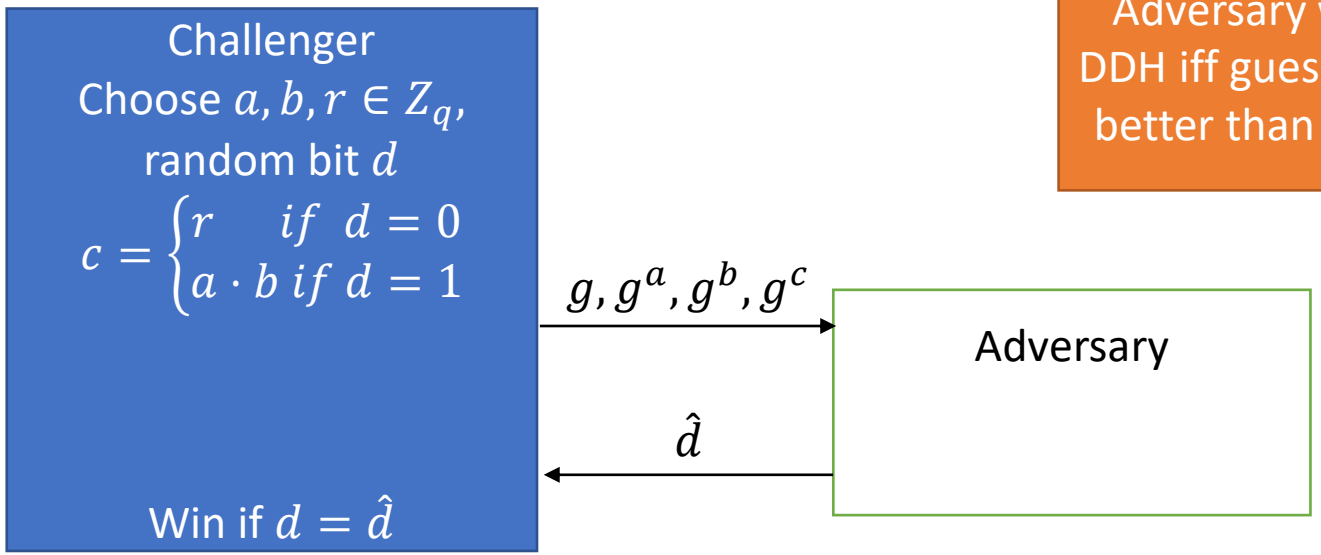
Decisional Diffie Hellman Problem (DDH)

Fix large primes p, q where $q|p-1$

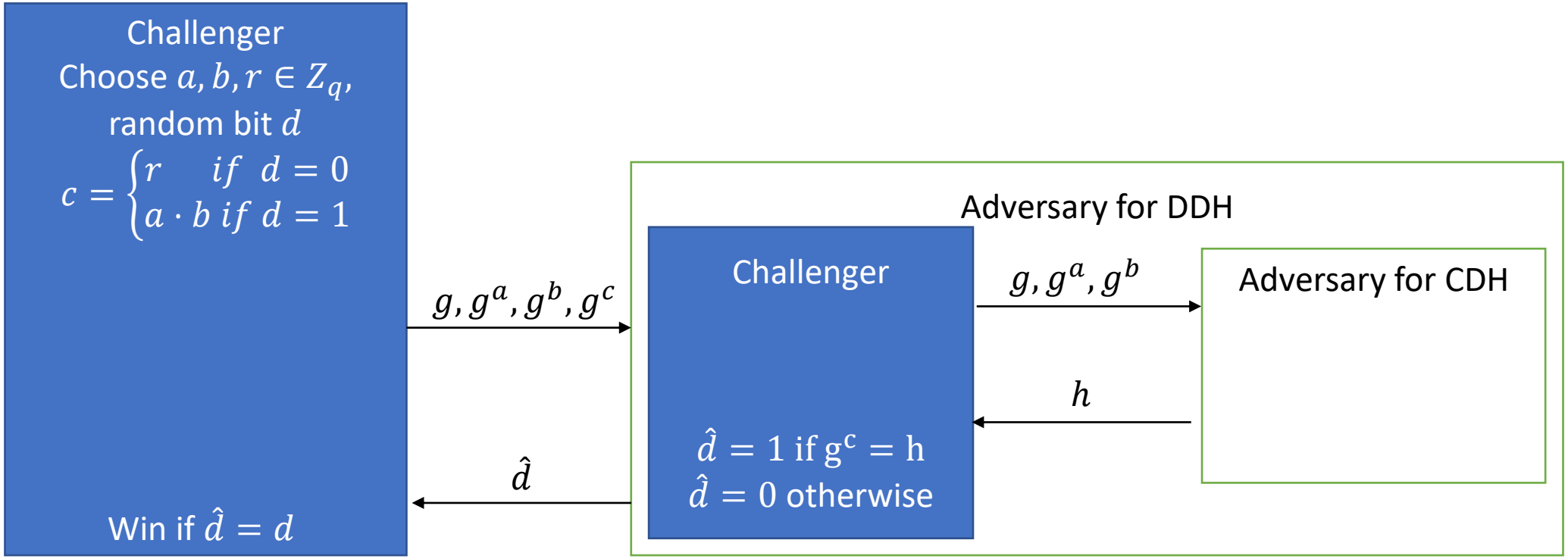
Fix $g \in Z_p^*$ such that g has order q

Guessing is correct with 50% chance!

Adversary wins DDH iff guesses >> better than 50%!



DDH vs. CDH

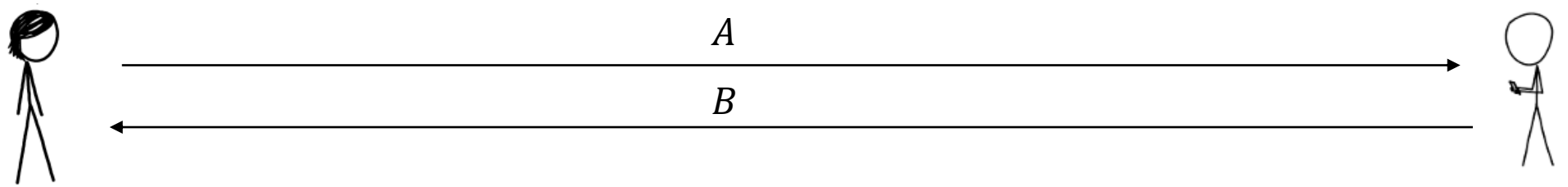


Reverse is not known in general.

Security of Diffie Hellman

Fix large primes p, q where $q|p-1$

Fix $g \in Z_p^*$ such that g has order q



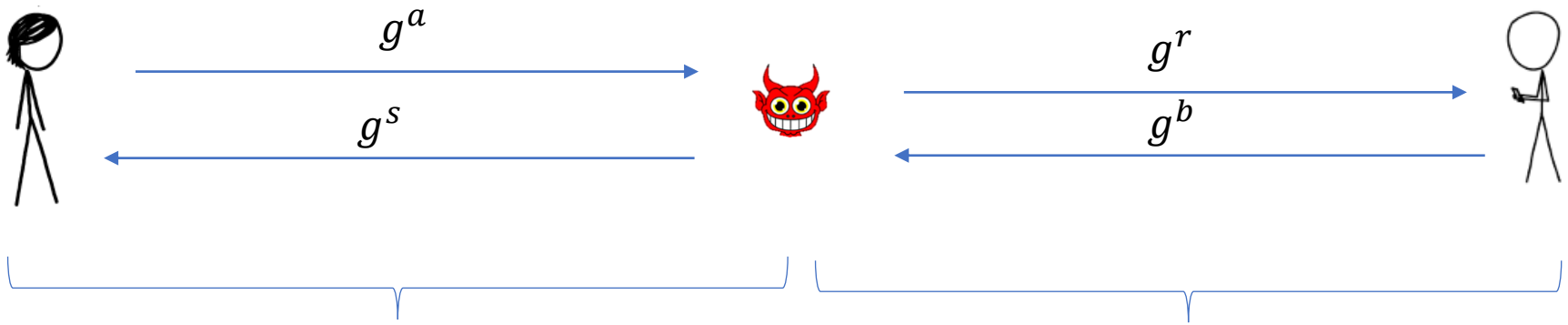
1. Choose random $a \in Z_q$
2. Compute $A = g^a \ mod \ p$
3. Output $k = B^a \ mod \ p$

Assuming CDH, no attacker can efficiently compute k

Assuming DDH, no attacker can efficiently distinguish k from a random group element

1. Choose random $b \in Z_q$
2. Compute $B = g^b \ mod \ p$
3. Output $k = A^b \ mod \ p$

Diffie Hellman and active attacks



$c_1 = Enc_{k_1}(hello\ bob)$

$c_2' = Enc_{k_1}(hello\ alice)$

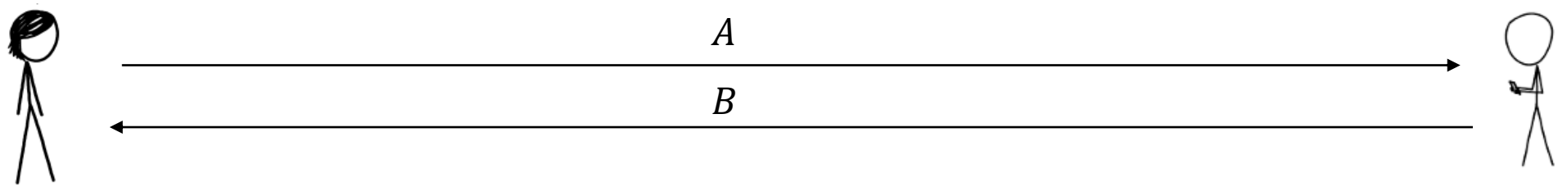
$c_1' = Enc_{k_2}(hello\ bob)$

$c_2 = Enc_{k_2}(hello\ alice)$

Diffie Hellman key agreement - generalized

Fix a large group G of prime order, generator $g \in G$

It must be hard to compute a given G, g, g^a

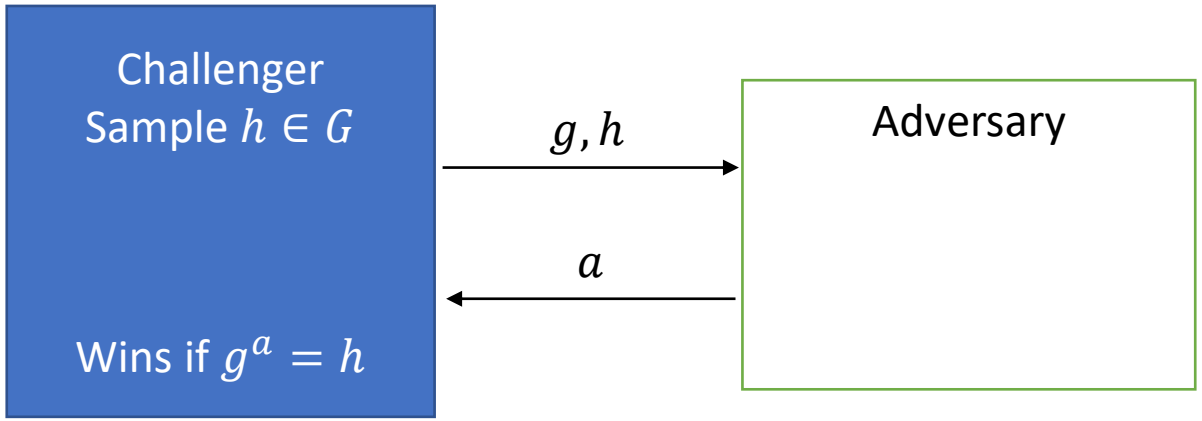


1. Choose random $a \in Z_{|G|}$
2. Compute $A = g^a$
3. Output $k = B^a$

1. Choose random $b \in Z_{|G|}$
2. Compute $B = g^b$
3. Output $k = A^b$

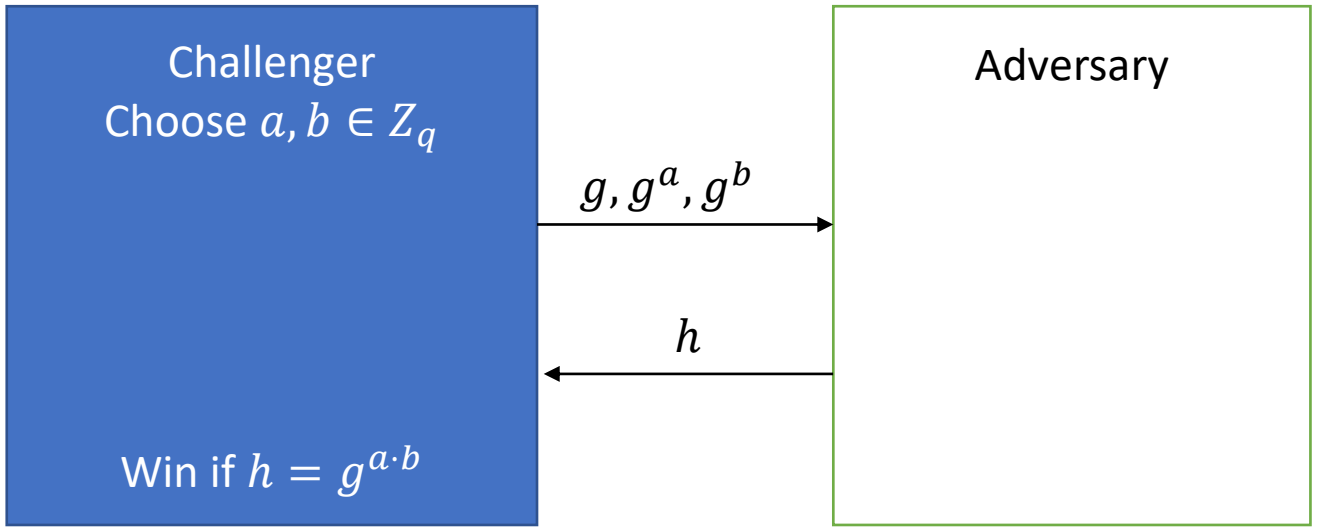
Generalized DLOG

Fix a large group G of prime order q, generator $g \in G$



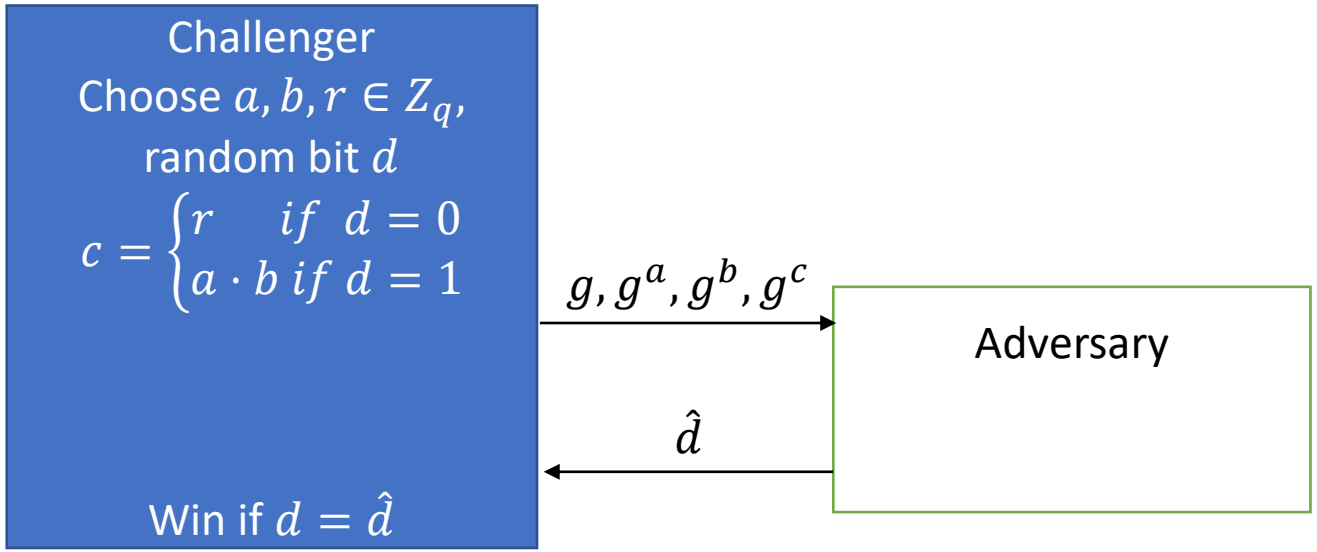
Generalized CDH

Fix a large group G of prime order q, generator $g \in G$

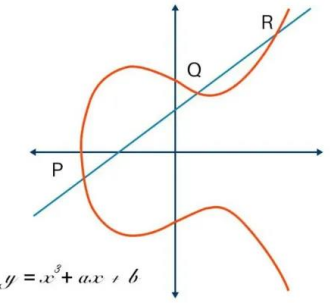


Generalized DDH

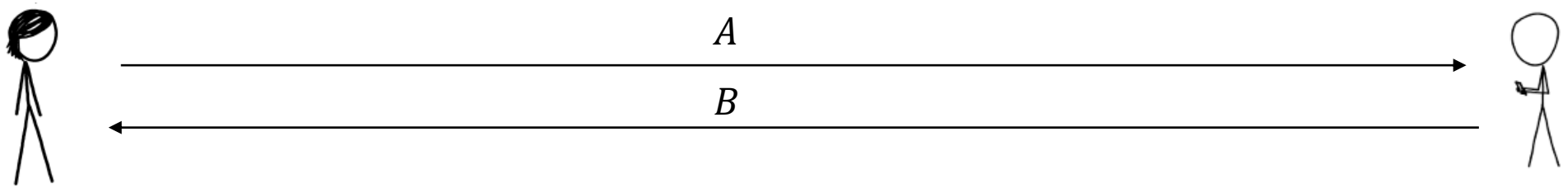
Fix a large group G of prime order q, generator $g \in G$



Diffie Hellman in practice



We saw: $\log_2(p)$ in 1000s of bits



<u>Used in practice:</u>
so-called Elliptic-curve groups (NIST curves, EC25519)

They deliver 128 bit security, but A, B only ≈ 260 bits long

How does ECC work?

Let K be any field not of characteristic 2,3 and $a, b \in K$.

Then the solutions (X, Y) of $E: Y^2 = X^3 + aX + b$ form a group.

In particular, if $K = F_q$ with $q = p^n, p > 3$ where $4a^3 \neq 27b^2$ then $|E(K)|$ has order $[q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q}]$

The group law if $p > 3$

Let $E: Y^2 = X^3 + aX + b$ with $a, b \in F_q$. Assume the existence of a point O.

Define $P_1 + O = O + P_1 = O$ and $P_1 - P_1 = O$

If $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ then $-P_1 = (x_1, -y_1)$

If $x_1 \neq x_2$ then $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$

If $x_1 = x_2$ and $y_1 \neq 0$ then $\lambda = \frac{3x_1^2 + a}{2y_1}$

Then $P_3 = P_1 + P_2 \neq O$ is given by

$$x_3 = \lambda^2 - x_1 - x_2$$
$$y_3 = (x_1 - x_3)\lambda - y_1$$

EC group has additive group law

Let $P \in E(F_q)$ then define

$$[m]P = \underbrace{P + \cdots + P}_{m \text{ times}}$$

ECDLP:

Given $E(F_q), P, [m]P$ it is hard to recover m

Example

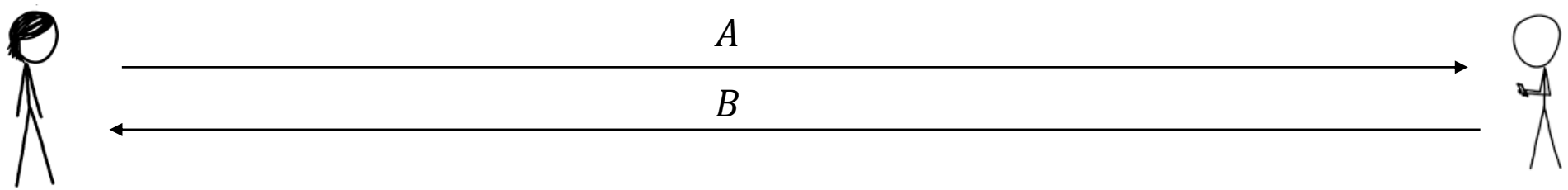
Let $q = 7, a = 1, b = 3$
$E: Y^2 = X^3 + X + 3$

+	O	$(4,1)$	$(6,6)$	$(5,0)$	$(6,1)$	$(4,6)$
O	O	$(4,1)$	$(6,6)$	$(5,0)$	$(6,1)$	$(4,6)$
$(4,1)$	$(4,1)$	$(6,6)$	$(5,0)$	$(6,1)$	$(4,6)$	O
$(6,6)$	$(6,6)$	$(5,0)$	$(6,1)$	$(4,6)$	O	$(4,1)$
$(5,0)$	$(5,0)$	$(6,1)$	$(4,6)$	O	$(4,1)$	$(6,6)$
$(6,1)$	$(6,1)$	$(4,6)$	O	$(4,1)$	$(6,6)$	$(5,0)$
$(4,6)$	$(4,6)$	O	$(4,1)$	$(6,6)$	$(5,0)$	$(6,1)$

If $P = (4,1)$ then

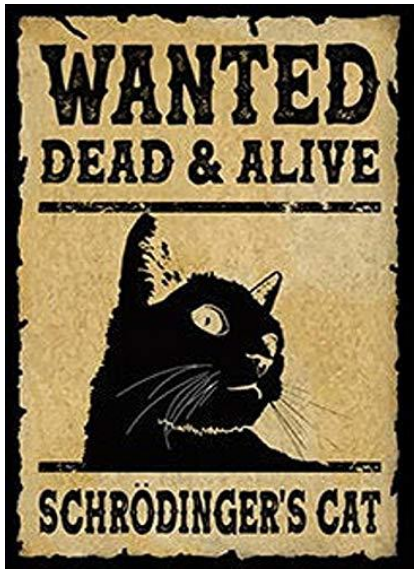
$$[2]P = (6,6)$$
$$[3]\mathrm{P} = (5,0)$$
$$[4]\mathrm{P} = (6,1)$$
$$[5]\mathrm{P} = (4,6)$$
$$[6]\mathrm{P} = O$$

Diffie Hellman



<u>Caveat:</u>

Any Diffie-Hellman ($mod\ p$, Elliptic curve) not secure against quantum computers



Summary

1. The Discrete Logarithm Problem
2. Diffie Hellman Key Exchange
3. The CDH and DDH problems