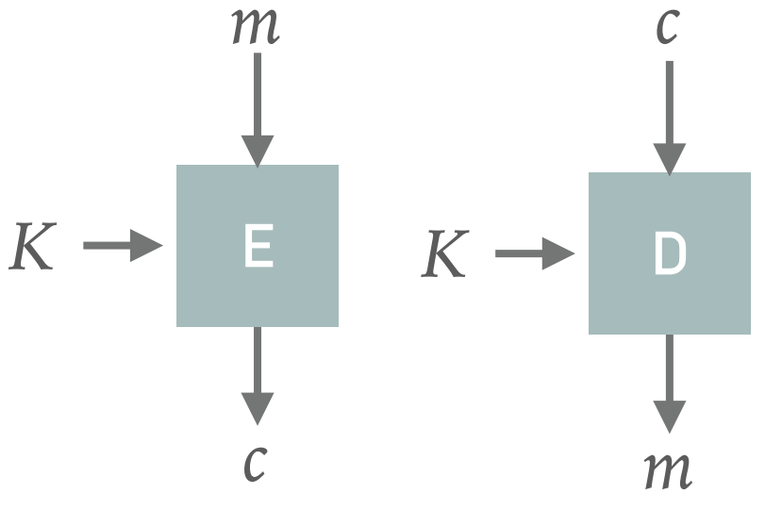
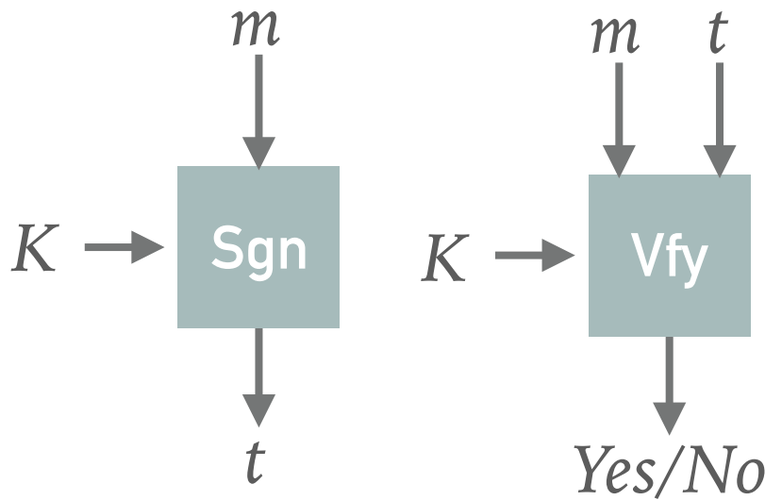
PUBLIC KEY CRYPTO

GRAD SEC

OCT 26 2017

RECAP





CONFIDENTIALITY

Block ciphers

Deterministic ⟹ use IVs

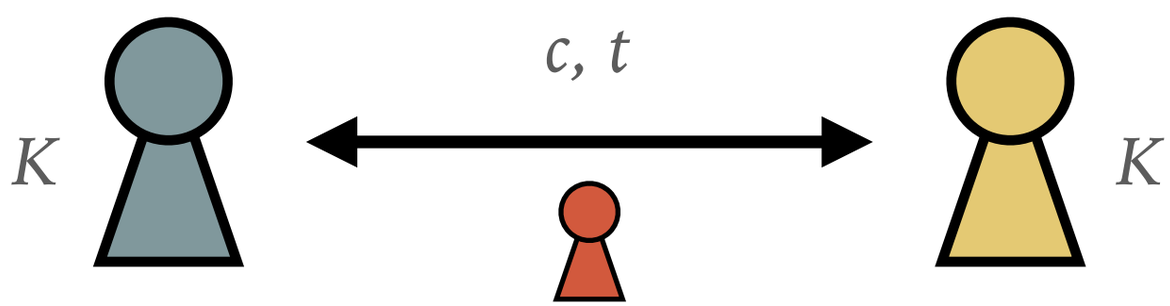
Fixed block size ⟹ use encryption "modes"

INTEGRITY

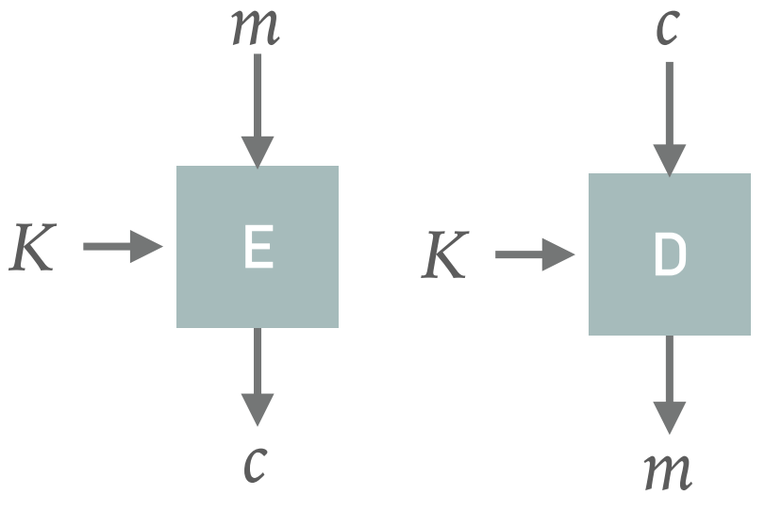
Message Authentication Codes (MACs)

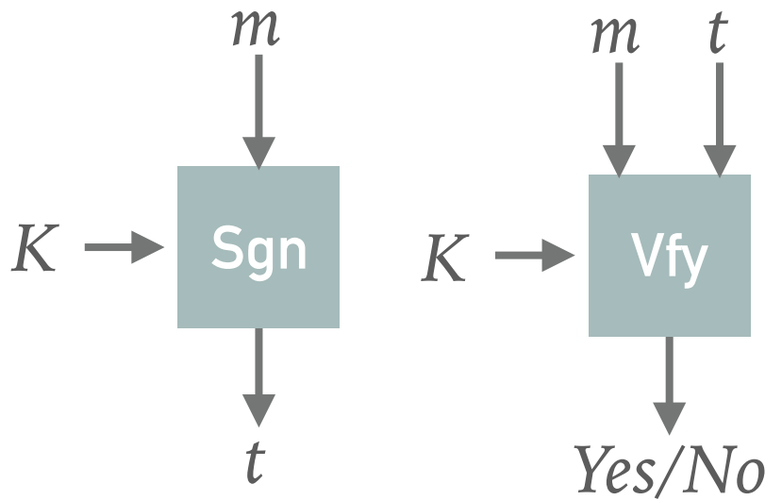
Send (message, tag) pairs

Verify that they match



RECAP





Today:

How do we establish K?

How do we know with whom we are communicating?

CONFIDENTIALITY

Block ciphers

Deterministic ⟹ use IVs

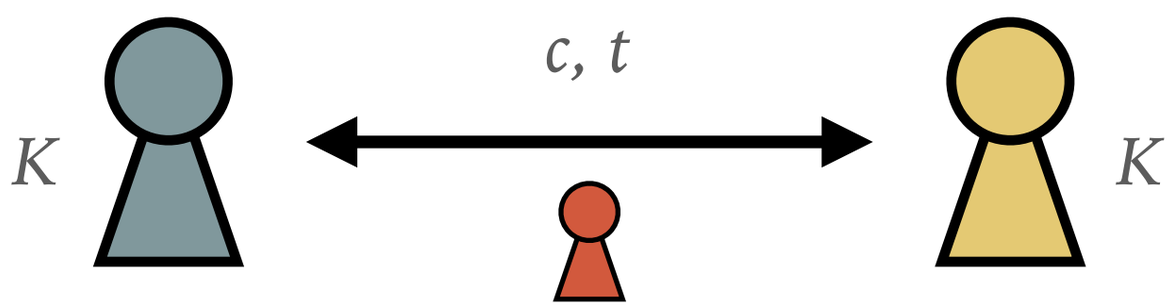
Fixed block size ⟹ use encryption "modes"

INTEGRITY

Message Authentication Codes (MACs)

Send (message, tag) pairs

Verify that they match



BLACKBOX #4:
DIFFIE HELLMAN KEY ESTABLISHMENT

HIGH-LEVEL REVIEW OF MODULAR ARITHMETIC

$x \bmod N$

HIGH-LEVEL REVIEW OF MODULAR ARITHMETIC

$x \bmod N$

g is a generator of mod N if
$\{1, 2, \ldots, N\text{-}1\} = \{g^0 \bmod N, g^1 \bmod N, \ldots, g^{N\text{-}2} \bmod N\}$

HIGH-LEVEL REVIEW OF MODULAR ARITHMETIC

$x \bmod N$

g is a generator of mod N if
$\{1, 2, \ldots, N\text{-}1\} = \{g^0 \bmod N, g^1 \bmod N, \ldots, g^{N\text{-}2} \bmod N\}$

$N=5, g=3$

$3^0 \bmod 5 = 1 \quad 3^1 \bmod 5 = 3 \quad 3^2 \bmod 5 = 4 \quad 3^3 \bmod 5 = 2$

HIGH-LEVEL REVIEW OF MODULAR ARITHMETIC

$x \bmod N$

g is a generator of mod N if
$\{1, 2, \ldots, N\text{-}1\} = \{g^0 \bmod N, g^1 \bmod N, \ldots, g^{N\text{-}2} \bmod N\}$

$N=5, g=3$

$3^0 \bmod 5 = 1 \quad 3^1 \bmod 5 = 3 \quad 3^2 \bmod 5 = 4 \quad 3^3 \bmod 5 = 2$

Given x and g, it is efficient to compute
$g^x \bmod N$

HIGH-LEVEL REVIEW OF MODULAR ARITHMETIC

$x \bmod N$

g is a generator of mod N if
$\{1, 2, \ldots, N\text{-}1\} = \{g^0 \bmod N, g^1 \bmod N, \ldots, g^{N\text{-}2} \bmod N\}$

$N=5, g=3$

$3^0 \bmod 5 = 1 \quad 3^1 \bmod 5 = 3 \quad 3^2 \bmod 5 = 4 \quad 3^3 \bmod 5 = 2$

Given x and g, it is efficient to compute
$g^x \bmod N$

Given g and g^x, it is efficient to compute x
(simply take $\log_g g^x$)

HIGH-LEVEL REVIEW OF MODULAR ARITHMETIC

$x \bmod N$

g is a generator of mod N if
$\{1, 2, \ldots, N\text{-}1\} = \{g^0 \bmod N, g^1 \bmod N, \ldots, g^{N\text{-}2} \bmod N\}$

$N=5, g=3$

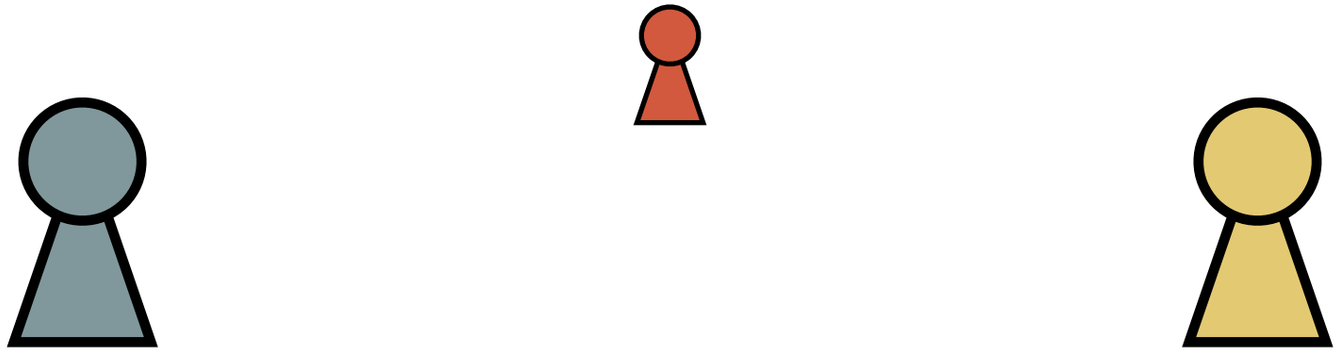
$3^0 \bmod 5 = 1 \quad 3^1 \bmod 5 = 3 \quad 3^2 \bmod 5 = 4 \quad 3^3 \bmod 5 = 2$

Given x and g, it is efficient to compute
$g^x \bmod N$

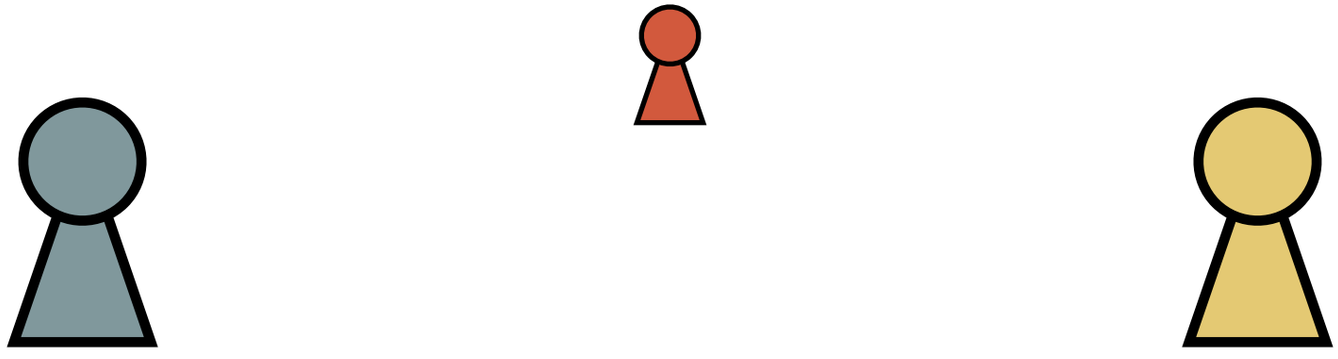
Given g and g^x, it is efficient to compute x
(simply take $\log_g g^x$)

Given g and g^x mod N it is *infeasible* to compute x
Discrete log problem

DIFFIE-HELLMAN KEY EXCHANGE

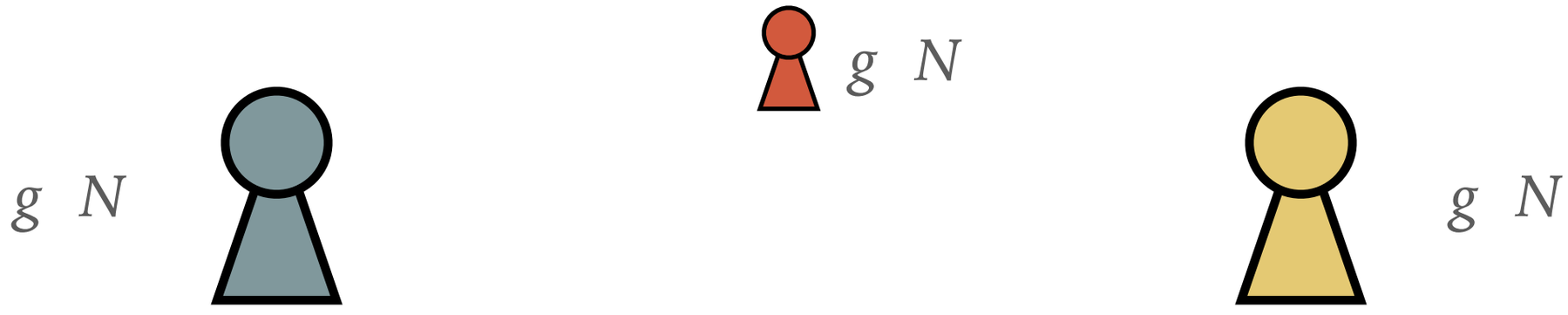


DIFFIE–HELLMAN KEY EXCHANGE



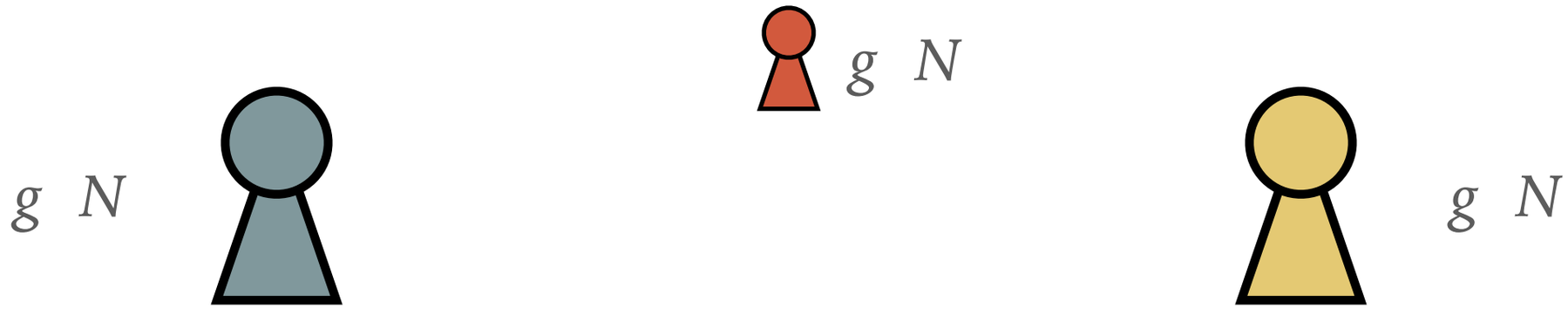
Public knowledge: g and N

DIFFIE–HELLMAN KEY EXCHANGE



Public knowledge: g and N

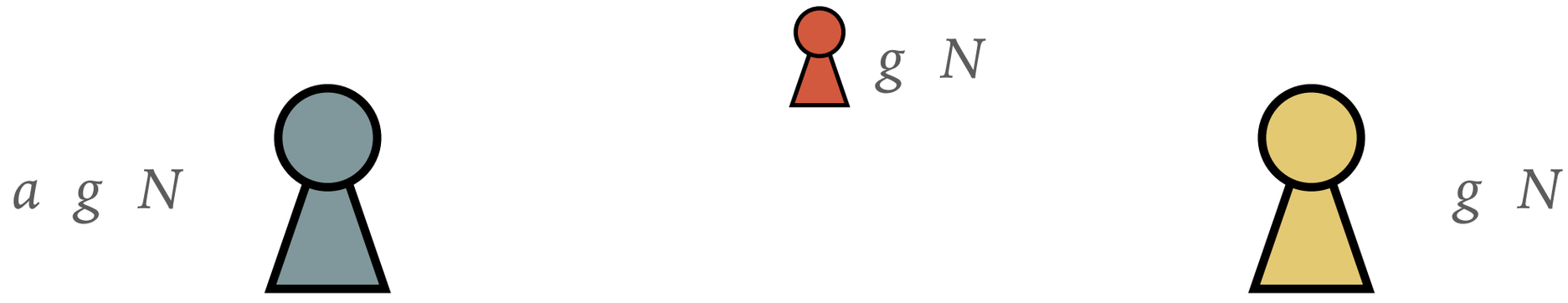
DIFFIE–HELLMAN KEY EXCHANGE



Public knowledge: g and N

Pick random a

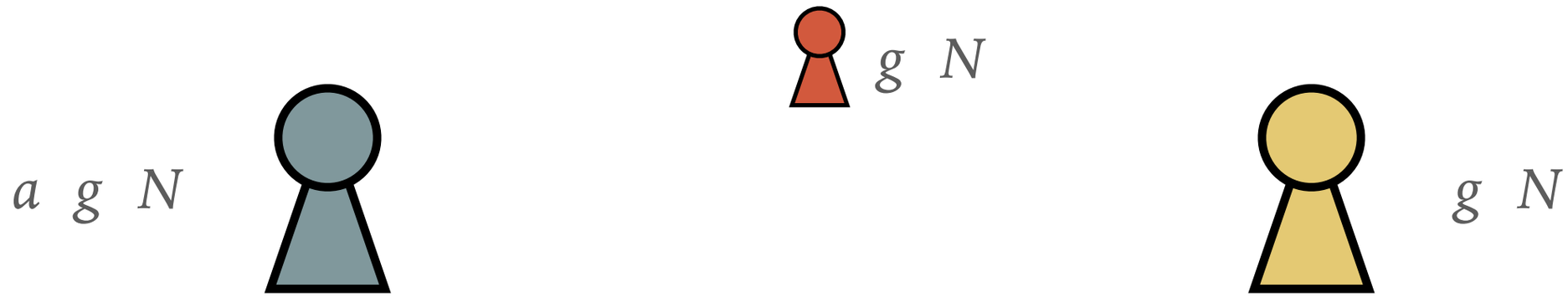
DIFFIE–HELLMAN KEY EXCHANGE



Public knowledge: g and N

Pick random a

DIFFIE–HELLMAN KEY EXCHANGE

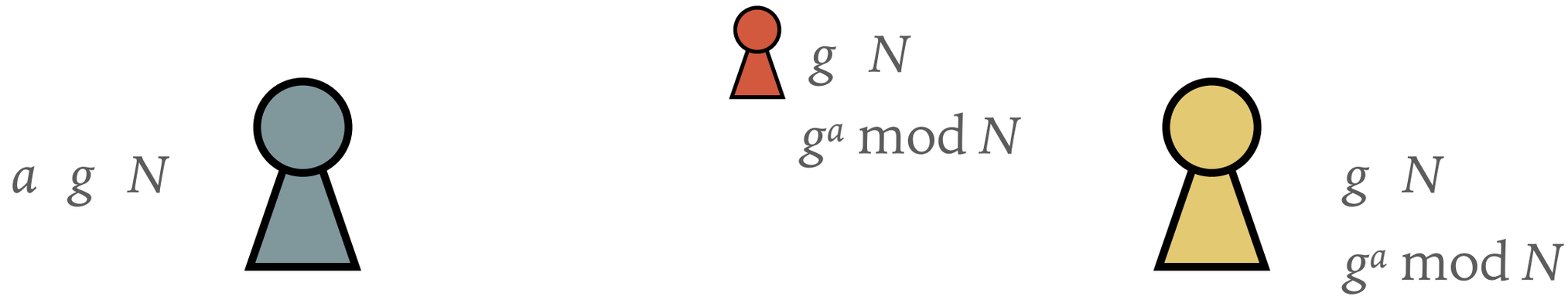


Public knowledge: g and N

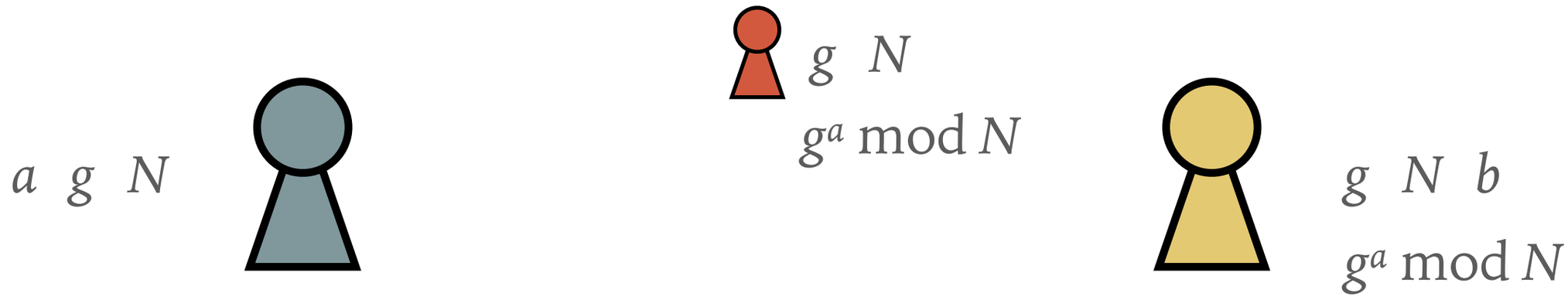
Pick random a

$g^a \bmod N$

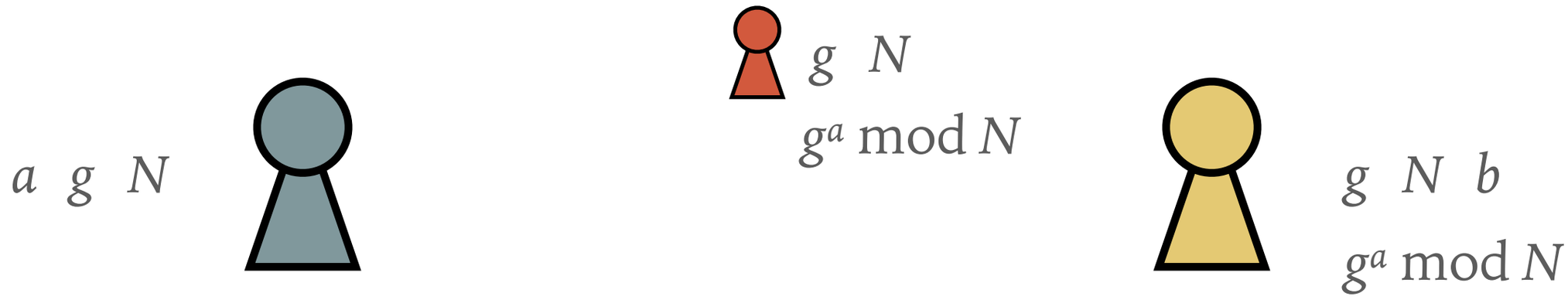
DIFFIE–HELLMAN KEY EXCHANGE



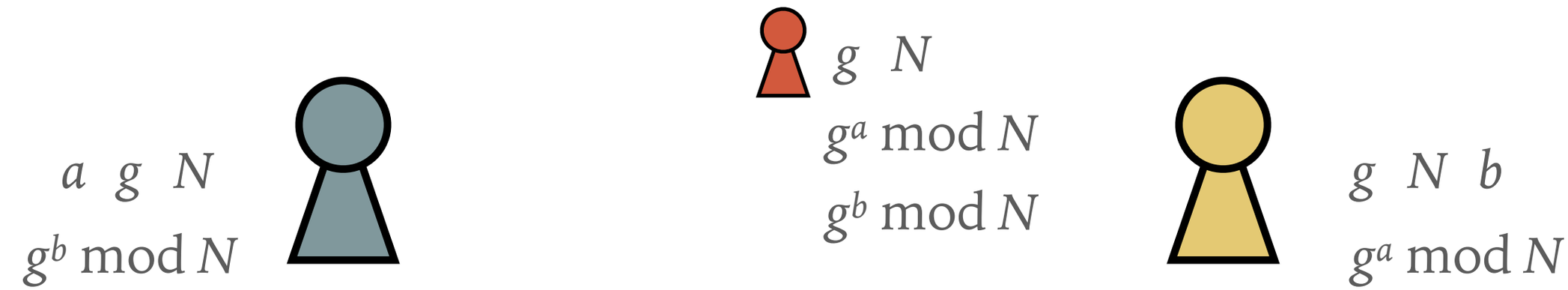
DIFFIE–HELLMAN KEY EXCHANGE



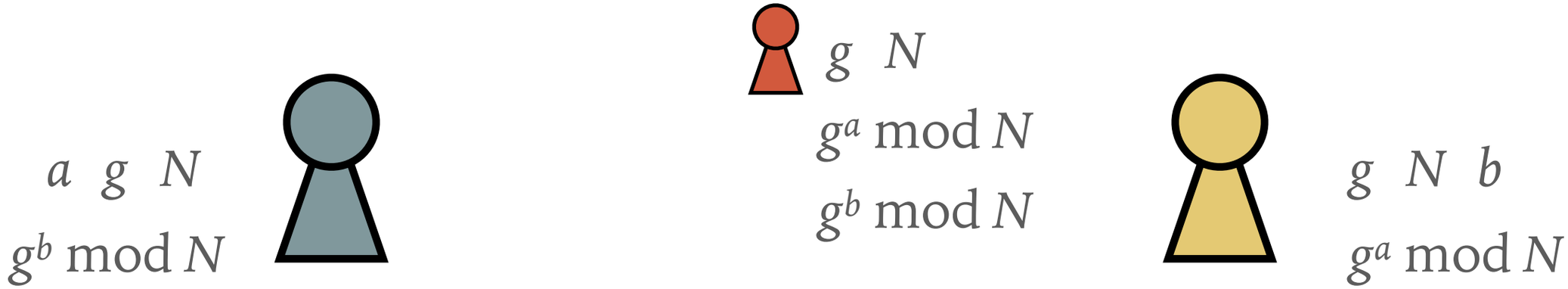
DIFFIE–HELLMAN KEY EXCHANGE



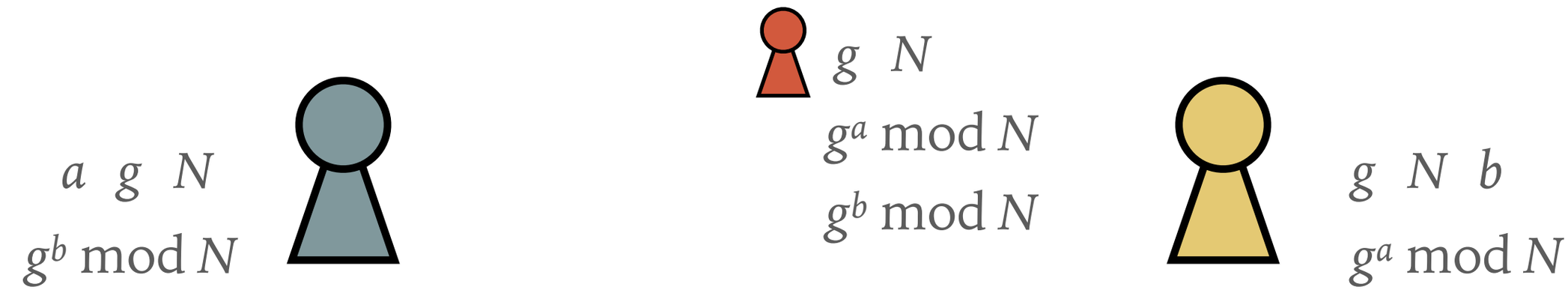
DIFFIE–HELLMAN KEY EXCHANGE



DIFFIE–HELLMAN KEY EXCHANGE



DIFFIE–HELLMAN KEY EXCHANGE



DIFFIE-HELLMAN KEY EXCHANGE

$g \quad N$

$g^a \bmod N$

$g^b \bmod N$

$g^{ab} \bmod N$

$$g^a \bmod N * g^b \bmod N \quad = g^{a+b} \bmod N$$

DIFFIE-HELLMAN KEY EXCHANGE

$g \quad N$

$g^a \bmod N$

$g^b \bmod N$

$g^{ab} \bmod N$

Given g and $g^x \bmod N$ it is *infeasible* to compute x

Discrete log problem

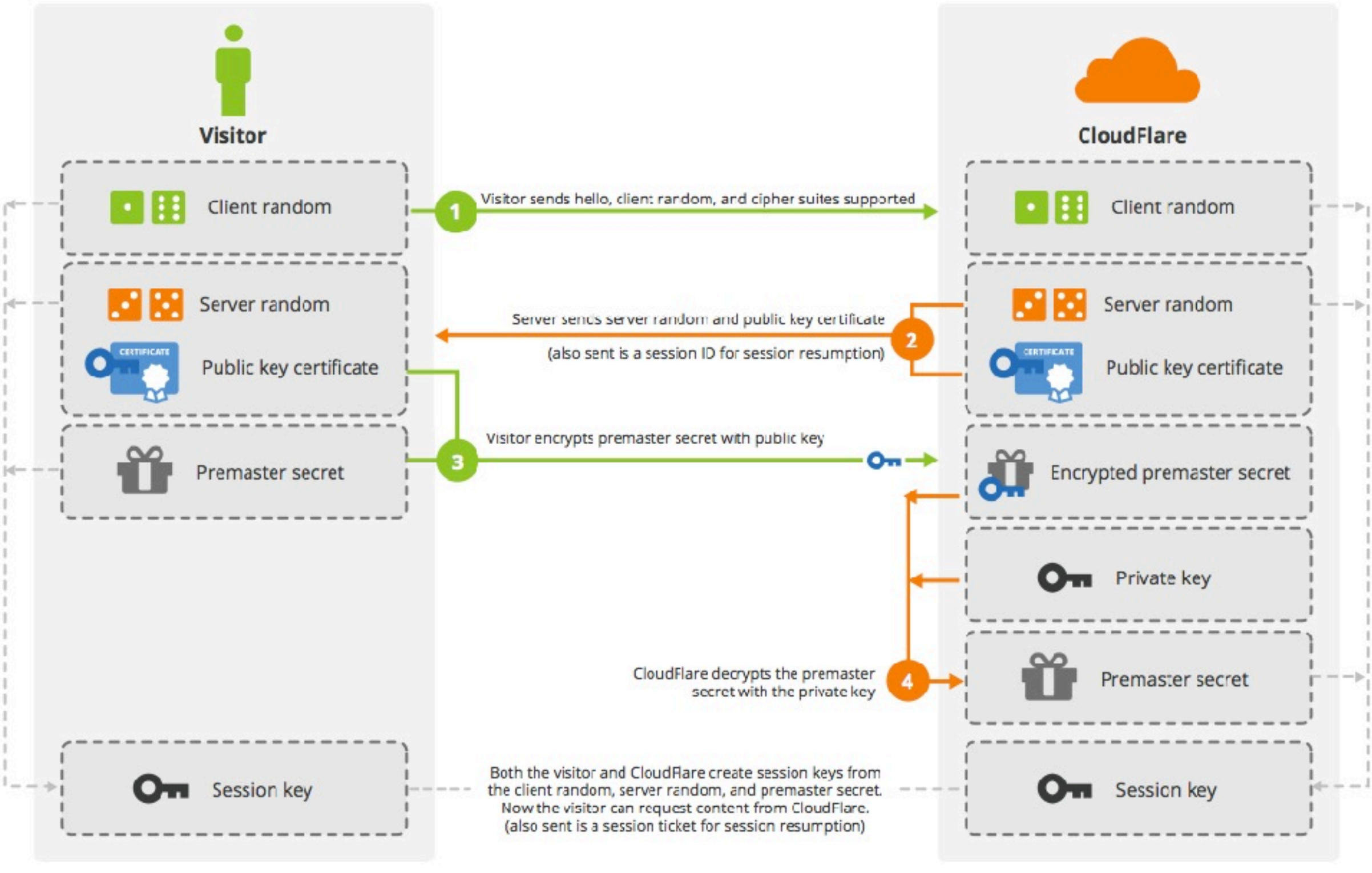
$$g^a \bmod N * g^b \bmod N \quad = g^{a+b} \bmod N$$

BLACKBOX #5:
PUBLIC KEY CRYPTOGRAPHY

PUTTING IT ALL TOGETHER:
PUBLIC KEY INFRASTRUCTURE (PKI)

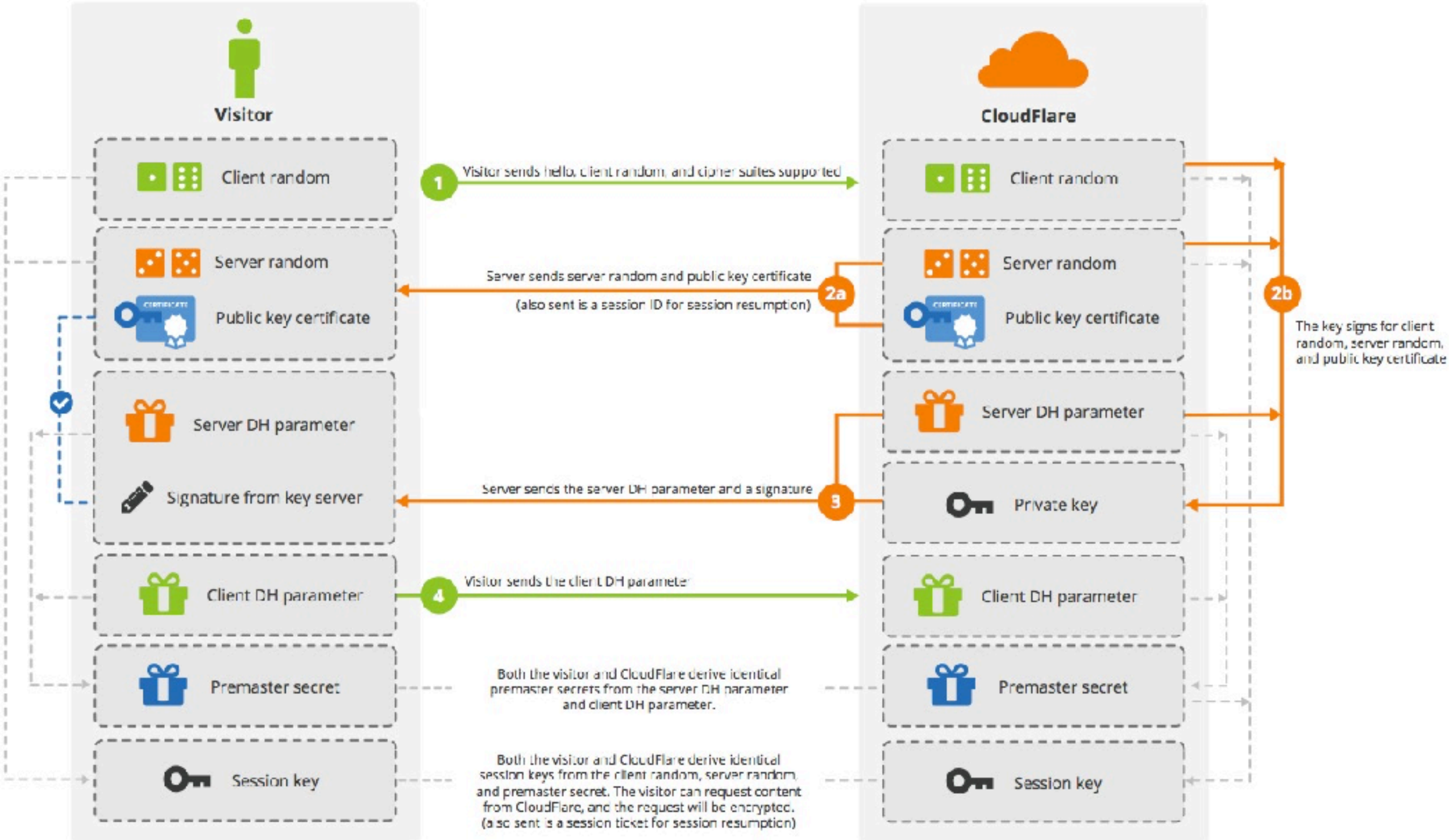
SSL Handshake (RSA) Without Keyless SSL

Handshake



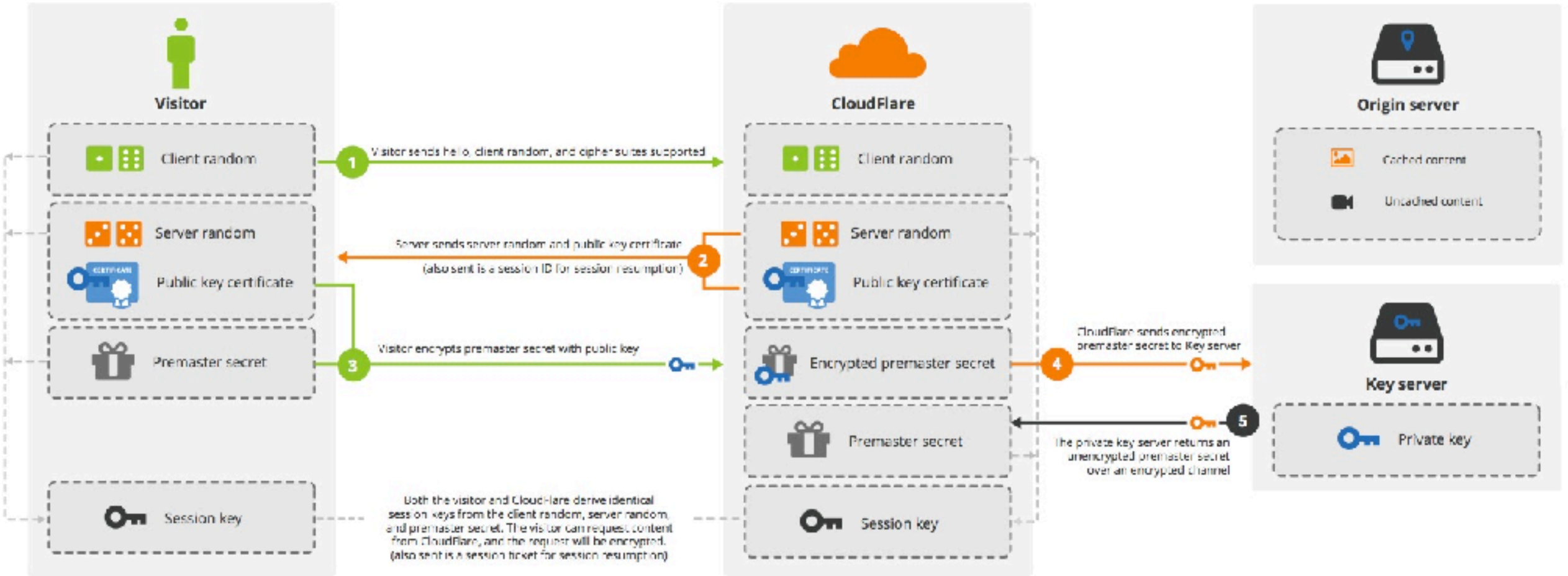
SSL Handshake (Diffie-Hellman) Without Keyless SSL

Handshake



CloudFlare Keyless SSL (RSA)

Handshake



CloudFlare Keyless SSL (Diffie-Hellman)

Handshake