Lecture 9 – Diffie-Hellman key exchange II, computational aspects

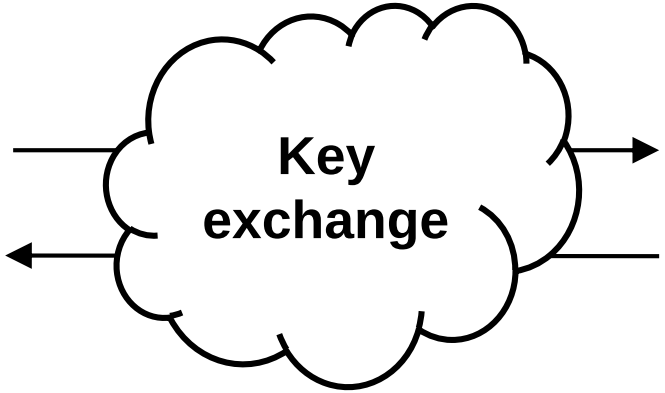
TEK4500

20.10.2020

Håkon Jacobsen

hakon.jacobsen@its.uio.no

Diffie-Hellman



Diffie-Hellman

$G = \langle g \rangle$ ← public

$A = g^a$ →

← $B = g^b$

$a \xleftarrow{\$} \{1, \dots, |G|\}$

$b \xleftarrow{\$} \{1, \dots, |G|\}$

$Z \leftarrow B^a = g^{ab}$

$Z \leftarrow A^b = g^{ab}$

Examples:

$G = (\boldsymbol{Z}_p^*, \cdot)$

$G = (E(\boldsymbol{Z}_p), +)$

Why is $(Z_p^*, \cdot)$ a group?

- $Z_p^* = \{1, 2, \ldots, p-1\}$
- Associativity ✓ $(a \cdot b) \cdot c = a \cdot (b \cdot c) \bmod p$
- Identity ✓ $1 \cdot a = a \cdot 1 = a \bmod p$
- Inverses ?

Definition: A **group** $(G, \circ)$ …

$\mathcal{G}1$: $(a \circ b) \circ c = a \circ (b \circ c)$ (associativity)
$\mathcal{G}2$: $\exists e \in G: e \circ a = a \circ e = a$ (identity)
$\mathcal{G}3$: $\exists a^{-1} \in G: a \circ a^{-1} = a^{-1} \circ a = e$ (inverses)

How to actually find a^{-1}?
Extended Euclidian Algorithm

Given $a \in Z_p^*$ can we always find $a^{-1} \in Z_p^*$?

Need to solve: $a \cdot x = 1 \bmod p$

Claim: $\exists m, n \in Z$ such that $ma + np = 1 \implies ma = 1 - np = 1 \bmod p$
$\implies a^{-1} = m \bmod p \in Z_p^*$

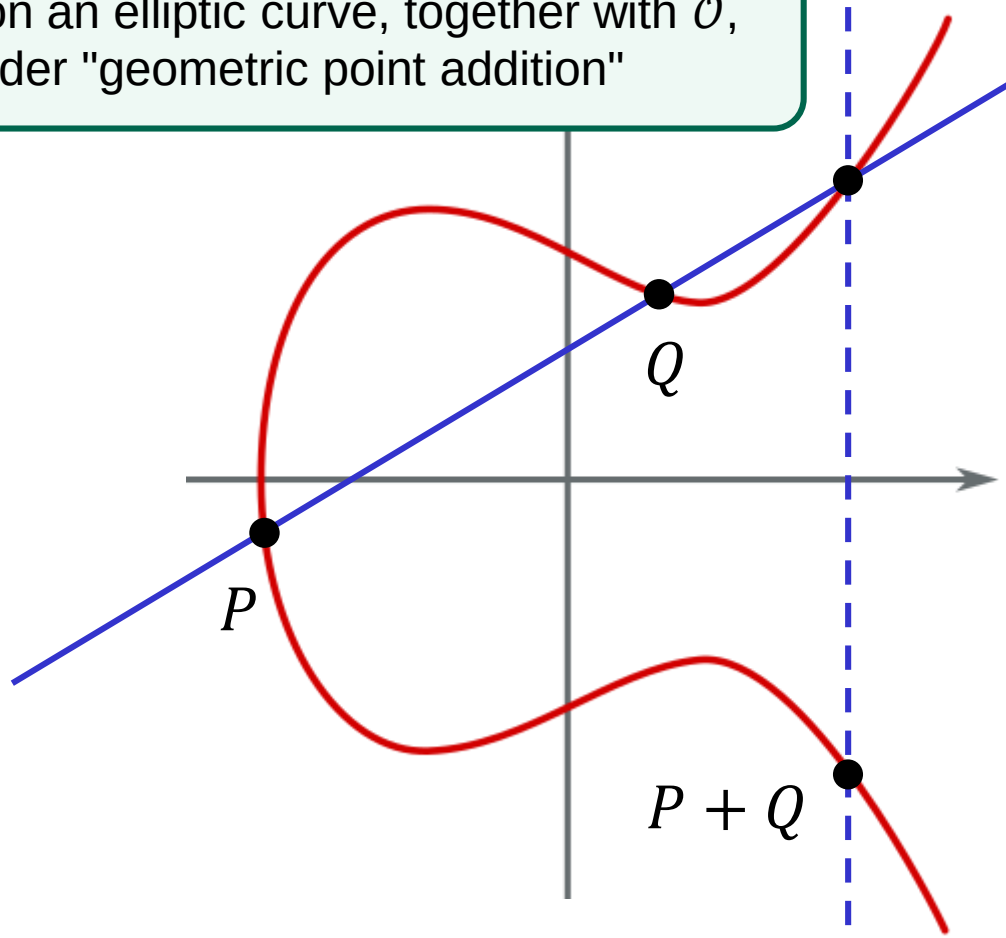
Proof: $I = \{sa + tp \mid s, t \in Z\}$

1) I contains a *positive* integer (e.g. a and p)
2) I contains a *smallest* positive integer $d = ma + np$
3) $p = qd + r \quad 0 \le r < d$
4) $r = p - qd = p - q(ma + np) = -qma + (1 - qn)p \in I$ (since d is the smallest positive integer in I)
5) $r = 0$ (since p is prime and $d \le a < p$)
6) $p = qd \implies d = 1$
7) $1 = ma + np$ Q.E.D

NON-CONSTRUCTIVE

Elliptic curves

Theorem: the points on an elliptic curve, together with $\mathcal{O}$, is an abelian group under "geometric point addition"



$$y^2 = x^3 + ax + b$$

$$a, b, x, y \in \boldsymbol{Z}_p$$

$$P + Q = (x_1, y_1) + (x_2, y_2) = (x_3, y_3)$$

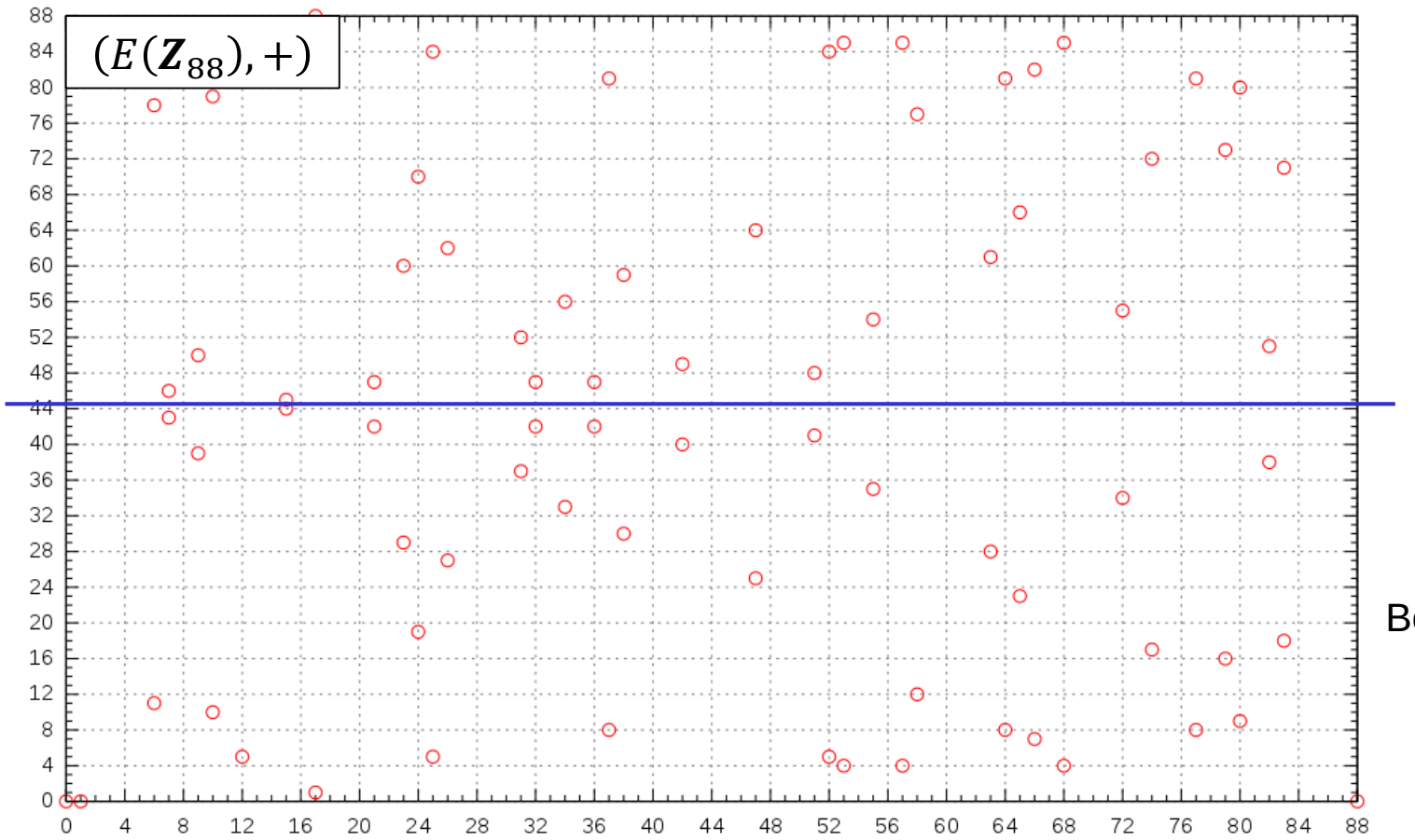
$$\begin{cases} x_3 = \dfrac{(x_1x_2 - 2a)x_1x_2 - 4b(x_1 + x_2) + a^2}{(x_1x_2 + a)(x_1 + x_2) + 2y_1y_2 + 2b} \\ y_3 = \dfrac{x_1x_2(x_1 + x_2) - x_3\big((x_1 + x_2)^2 - x_1x_2 + a\big) - y_1y_2 - b}{y_1 + y_2} \end{cases}$$

Still valid!

Elliptic curves over finite fields

Theorem: the points on an elliptic curve, together with $\mathcal{O}$, is an abelian group under "geometric point addition"

Notation: $(E(\boldsymbol{Z}_p), +)$ = an elliptic curve group defined over $\boldsymbol{Z}_p$



$$y^2 = x^3 + ax + b \pmod{p}$$

$$a, b, x, y \in \boldsymbol{Z}_{88}$$

$$P + Q = (x_1, y_1) + (x_2, y_2) = (x_3, y_3)$$

$$\begin{cases} x_3 = \dfrac{(x_1x_2 - 2a)x_1x_2 - 4b(x_1 + x_2) + a^2}{(x_1x_2 + a)(x_1 + x_2) + 2y_1y_2 + 2b} \\ y_3 = \dfrac{x_1x_2(x_1 + x_2) - x_3\left((x_1 + x_2)^2 - x_1x_2 + a\right) - y_1y_2 - b}{y_1 + y_2} \end{cases}$$

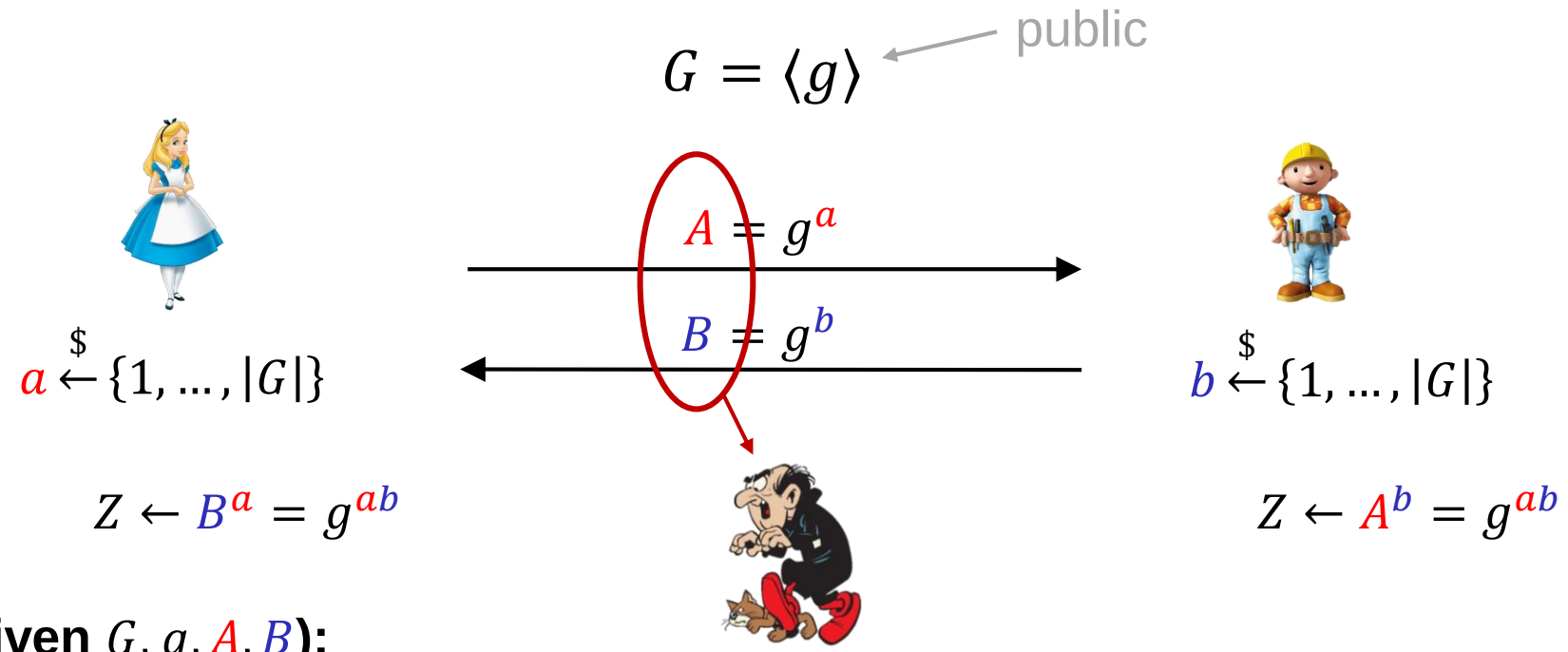
Both addition *and* multiplication needed mod p

Need $(\boldsymbol{Z}_p, +)$ *and* $(\boldsymbol{Z}_p^*, \cdot)$

⇓

Finite field: $(\boldsymbol{F}_p, +, \cdot)$

Diffie-Hellman – security



Security (given G, g, A, B):

- Must be hard to compute $Z \leftarrow g^{ab}$ (DH assumption)
- Must be hard to find a (or b) (DLOG assumption)

- $G = (\boldsymbol{Z}_p, +)$ not secure
- $G = (\boldsymbol{Z}_p^*, \cdot)$ secure* for p large enough (conjectured)
- $G = (E(\boldsymbol{F}_p), +)$ secure* for $|E(\boldsymbol{F}_p)|$ large enough (conjectured)

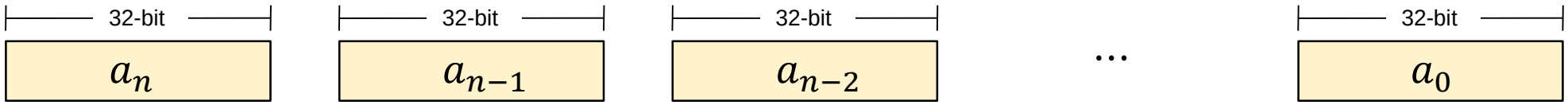
*Many caveats

Large enough?

$$p = 171254583176141379301960419792575778264088323240375085733932929816426671$$
$$397476217788024387752387285929683446135893799323484756135034769321631669$$
$$738132186983438164632891441853629126025225404949830905314972329658295365$$
$$245072698488256583114202993359222957097432675083225259667739503949192575$$
$$768420387716327420441424710535098501236058838158571626669177751934961573$$
$$726561955583057270098912760065140004093658772181713883199238963093777917$$
$$625906143118496429613802248519404604217104493689272529748703958739363879$$
$$096722748832953774810081504758785902705917983505634881680809238046118223$$
$$875201980540029906239114543891047740921 83 \approx 2^{2048}$$

Big-number arithmetic

a = 2048-bit integer, 64-bit CPU



Algorithm	Input	Output	Time
ADD	a, b	$a + b$	$\mathcal{O}(n)$
MULT	a, b	ab	$\mathcal{O}(n^2)$
INT-DIV	a, b	(q, r) s.t. $a = qb + r$ and $0 \leq r < b$	$\mathcal{O}(n^2)$
MOD	a, p	$a \bmod p$	$\mathcal{O}(n^2)$
MOD-INV	$a \in \boldsymbol{Z}_p^*$	$a^{-1} \in \boldsymbol{Z}_p^*$	$\mathcal{O}(n^2)$

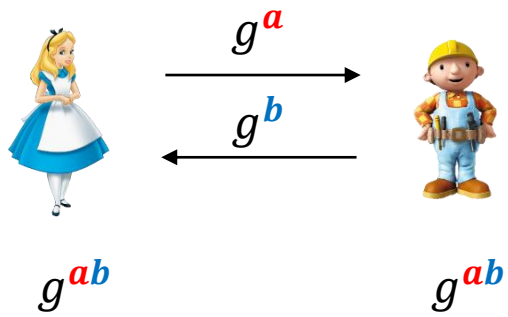
$\mathcal{O}(n \log n)$*

*all numbers are n bits

* $n > 2^{7137398073256634897664758526207831206 41}$

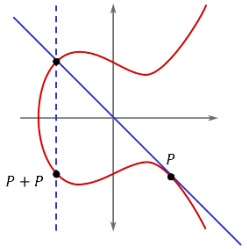
Diffie-Hellman – computations

- $(\boldsymbol{Z}_p^*, \cdot)$
  - Find prime p (one-time)
  - Find generator $\langle g \rangle = (\boldsymbol{Z}_p^*, \cdot)$ (one-time)
  - Compute $g^a = gg \cdots g \mod p$
    - Multiply $x \cdot y \mod p$



Group exponentiation g^a

- $(E(\boldsymbol{F}_p), +)$
  - Find prime p (one-time)
  - Generate curve $y^2 = x^3 + ax + b \mod p$ (one-time)
  - Find curve group order $|E(\boldsymbol{F}_p)|$ (one-time)
  - Find generator P (one-time)
  - Compute $aP = P + P + \cdots + P$
    - Point addition



Diffie-Hellman – in $\left(Z_p^*,\cdot\right)$

$p =$
17125458317614137930196041979257577826408832324037508573393292981642667139747621778802438775238728592968344613589379932348475613503476932163166973813218698343816463289144185362912602522540494983090531497232965829
53652450726984882565831142029933592229570974326750832252596677395039491925757684203877163274204414247105350985012360588381585716266691777519349615737265619555830572700989127600651400040936587721817138831992389630
93777917625906143118496429613802248519404604217104493689272529748703958739363879096722748832953774810081504758759027059179835056348816808092380461182238752019805400299062391145438910477409218 3

$A = 2 \mod p$

323170060713110073003389139264238282488179412411402391
128420097514007417066343542226196894173635693471179017
379097041917546058732091950288537589861856221532121754
125149017745202702357960782362488842461894775876411059
286460994117232454266225221932305409190376805242355191
256797158701170010580558776510388618472802579760549035
697325615261670813393617995413364765591603683178967290
731783845896806396719009772021941686472258710314113364
293195361934716365332097170774482279885885653692086452
966360772502689555059283627511211740969729980684105543
595848665832916421362182310789909994486524682624169720
359118525070453610905 59

$\xleftarrow{\$} \{1 \dots p\}$

665680077810100734070476416898417408020670352441378967
997224101900193957211854827569676933273935982997835638
067380762809024311842715496660113976613131478051784487
322446809608196031803691263486170912693625523249742383
264476433978409434004770395167011614217279552198029936
108023398643999746539201834933168220864789880837484536
563067997761270826642223539437541791058416731683176995
365899867720283590420932417377927106884773199080517477
615608675490982255098980545292032908358093913531433702
049429047413071525556307299541445514389721222256380833
743627991333762777307118317040885305789910094293548481
550130956194277068752 4

$Z \leftarrow 2$

$\times$

$\mod p$

Recall

Theorem: if $(G,\circ)$ is a finite group, then for all $g \in G$:

$$g^{|G|} = e$$

Corollary I: $g^i = g^{i \bmod |G|}$

Corollary II (Lagrange's theorem):

if $H < G$ then the order of H divides the order of G (i.e $|H| \mid |G|$)

Diffie-Hellman – in a *subgroup* of $(Z_p^*,\cdot)$

$p =$ 1712545831761413793019604197925757782640883232403750857339329298164266713974762177880243877523872859296834461358937993234847561350347693216316697381321869834381646328914418536291260252254049498309053149723296582 9
5365245072698488256583114202993359222957097432675083225259667739503949192575768420387716327420441424710535098501236058838158571626669177751934961573726561955583057270098912760065140004093658772181713883199238963 0
9377791762590614311849642961380224851940460421710449368927252974870395873936387909672274883295377481008150475878590270591798350563488168080923804611822387520198054002990623911454389104774092183

$= 2 \cdot 7 \cdot 13 \cdot q_1 \cdot q_2 \cdot q_3 \cdot q_4 \cdot q_5 + 1$

$|\boldsymbol{Z}_p^*| = p - 1$

$H = \langle g \rangle < (\boldsymbol{Z}_p^*, \cdot)$

$|H| = q_4 \approx 2^{256}$

$=$ 6376235136497265356416 99
5292055104892632668341 8277
161756363136327793285 4227

$A = 2^{a} \bmod p$, with exponent:
32317006071311007300338913926423828248817941241140 2391
12842009751400741706634354222619689417363569347117 9017
37909704191754605873209195028853758986185622153212 1754
12514901774520270235796078236248884246189477587641 1059
28646099411723245426622522193230540919037680524235 5191
25679715870117001058055877651038861847280257976054 9035
69732561526167081339361799541336476559160368317896 7290
73178384589680639671900977202194168647225871031411 3364
29319536193471636533209717077448227988588565369208 6452
96636077250268955505928362751121174096972998068410 5543
59584866583291642136218231078990999448652468262416 9720
3591185250704536109055 9

$B = 2^{b} \bmod p$, with exponent:
66568007781010073407047641689841740802067035244137 8967
99722410190019395721185482756967693327393598299783 5638
06738076280902431184271549666011397661313147805178 4487
32244680960819603180369126348617091269362552324974 2383
26447643397840943400477039516701161421727955219802 9936
10802339864399974653920183493316822086478988083748 4536
56306799776127082664222353943754179105841673168317 6995
36589986772028359042093241737792710688477319908051 7477
61560867549098225509898054529203290835809391353143 3702
04942904741307152555630729954144551438972122225638 0833
74362799133376277730711831704088530578991009429354 8481
5501309561942770687524

Alice: exponent
32317006071311007300338913926423828248817941241140 2391
12842009751400741706634354222619689417363569347117 9017
37909704191754605873209195028853758986185622153212 1754
[illegible]
[illegible]522193230540919037680524235 5191
25679715870117001058055877651038861847280257976054 9035
69732561526167081339361799541336476559160368317896 7290
73178384589680639671900977202194168647225871031411 3364
29319536193471636533209717077448227988588565369208 6452
96636077250268955505928362751121174096972998068410 5543
59584866583291642136218231078990999448652468262416 9720
3591185250704536109055 9
$\overset{\$}{\leftarrow} \{1 \ldots p\}$ / $\{1 \ldots q_4\}$

Bob: exponent
66568007781010073407047641689841740802067035244137 8967
99722410190019395721185482756967693327393598299783 5638
06738076280902431184271549666011397661313147805178 4487
32244680960819603180369126348617091269362552324974 2383
29177641728484883278069152197089138002064929787753 5257
26447643397840943400477039516701161421727955219802 9936
36186058877137490281835
10802339864399974653920183493316822086478988083748 4536
56306799776127082664222353943754179105841673168317 6995
36589986772028359042093241737792710688477319908051 7477
61560867549098225509898054529203290835809391353143 3702
04942904741307152555630729954144551438972122225638 0833
74362799133376277730711831704088530578991009429354 8481
5501309561942770687524
$\overset{\$}{\leftarrow} \{1 \ldots p\}$ / $\{1 \ldots q_4\}$

Corollary I: $g^i = g^{i \bmod |H|}$

$Z \leftarrow 2^{a \times b} \bmod p$, with exponents:
32317006071311007300338913926423828248817941241140 2391
12842009751400741706634354222619689417363569347117 9017
37909704191754605873209195028853758986185622153212 1754
12514901774520270235796078236248884246189477587641 1059
28646099411723245426622522193230540919037680524235 5191
25679715870117001058055877651038861847280257976054 9035
69732561526167081339361799541336476559160368317896 7290
73178384589680639671900977202194168647225871031411 3364
29319536193471636533209717077448227988588565369208 6452
96636077250268955505928362751121174096972998068410 5543
59584866583291642136218231078990999448652468262416 9720
3591185250704536109055 9
$\times$
66568007781010073407047641689841740802067035244137 8967
99722410190019395721185482756967693327393598299783 5638
06738076280902431184271549666011397661313147805178 4487
32244680960819603180369126348617091269362552324974 2383
26447643397840943400477039516701161421727955219802 9936
10802339864399974653920183493316822086478988083748 4536
56306799776127082664222353943754179105841673168317 6995
36589986772028359042093241737792710688477319908051 7477
61560867549098225509898054529203290835809391353143 3702
04942904741307152555630729954144551438972122225638 0833
74362799133376277730711831704088530578991009429354 8481
5501309561942770687524

Diffie-Hellman – in a *subgroup* of $\left(Z_p^*,\cdot\right)$

$p =$ 1712545831761413793019604197925757782640883232403750857339329298164266713974762177880243877523872859296834461358937993234847561350347693216316697381321869834381646328914418536291260252254049498309053149723296582 9
5365245072698488256583114202993359222957097432675083225259667739503949192575768420387716327420441424710535098501236058838158571626669177751934961573726561955583057270098912760065140004093658772181713883199238963 0
937779176259061431184964296138022485194046042171044936892725297487039587393638790967227488329537748100815047587859027059179835056348816808092380461182238752019805400299062391145438910477409218 3

$= 2 \cdot 7 \cdot 13 \cdot q_1 \cdot q_2 \cdot q_3 \cdot q_4 \cdot q_5 + 1$

$H = \langle g \rangle < \left(\boldsymbol{Z}_p^*,\cdot\right)$

$|H| = q_4 \approx 2^{256}$

$=$ 6376235136497265356464169 9
5292055104892632668341827 7
161756363136327793285422 7

3705764346409644403258417782318102824858084594001093748750648996496347171581 6 $\xleftarrow{\$} \{1 \ldots q_4\}$

$A = g^{37057643464096444032584177823181028248580845940010937487506489964963471715816} \bmod p$ →

2917764172848488327806915219708913800206492978775352573618605887713749028183 5 $\xleftarrow{\$} \{1 \ldots q_4\}$

← $B = g^{29177641728484883278069152197089138002064929787753525736186058877137490281835} \bmod p$

Corollary I: $g^i = g^{i \bmod |H|}$

$Z \leftarrow 2$ 32317006071311007300338913926423828248817941241140239112842009751400741706634354222619689417363569347117901737909704191754605873209195028853758986185622153212175412514901774520270235796078236248884246189477587641105928646099411723245426622522193230540919037680524235519125679715870117001058055877651038861847280257976054903569732561526167081339361799541336476559160368317896729073178384589680639671900977202194168647225871031411336429319536193471636533209717077448227988588565369208645296636077250268955505928362751121174096972998068410554359584866583291642136218231078990999448652468262416972035911852507045361090559
$\times$ 66568007781010073407047641689841740802067035244137896799722410190019395721185482756967693327393598299783563806738076280902431184271549666011397661313147805178448732244680960819603180369126348617091269362552324974238326447643397840943400477039516701161421727955219802993610802339864399974653920183493316822086478988083748453656306799776127082664222353943754179105841673168317699536589986772028359042093241737792710688477319908051747761560867549098225509898054529203290835809391353143370204942904741307152555630729954144551438972122225638083374362799133376277730711831704088530578991009429354848155013095619427706875 24
$\bmod p$

Diffie-Hellman – in a *subgroup* of $(Z_p^*, \cdot)$

$$p = \begin{array}{l}171254583176141379301960419792575778264088323240375085733932929816426671397476217788024387752387285929683446135893799323484756135034769321631669738132186983438164632891441853629126025225404949830905314972329658 29\\ 536524507269848825658311420299335922295709743267508322525966773950394919257576842038771632742044142471053509850123605883815857162666917775193496157372656195558305727009891276006514000409365877218171388319923896 30\\ 9377917625906143118496429613802248519404604217104493689272529748703958739363879096722748832953774810081504758785902705917983505634881680809238046118223875201980540029906239114543891047740921 83\end{array}$$

$$= 2 \cdot 7 \cdot 13 \cdot q_1 \cdot q_2 \cdot q_3 \cdot q_4 \cdot q_5 + 1$$

$$H = \langle g \rangle < (\boldsymbol{Z}_p^*, \cdot)$$

$$|H| = q_4 \approx 2^{256}$$

$$= \begin{array}{l}6376235136497265356464169 9\\ 529205510489263266834182 77\\ 16175636313632779328542 27\end{array}$$

$$A = g^{\begin{array}{l}3705764346409644403258417782318102824858084594001093 74\\ 8750648996496347171581 6\end{array}} \bmod p$$

$$\begin{array}{l}3705764346409644403258417782318102824858084594001093 74\\ 8750648996496347171581 6\end{array} \overset{\$}{\leftarrow} \{1 \ldots q_4\}$$

$$\begin{array}{l}29177641728484883278069152197089138002064929787753525 7\\ 3618605887713749028183 5\end{array} \overset{\$}{\leftarrow} \{1 \ldots q_4\}$$

$$B = g^{\begin{array}{l}29177641728484883278069152197089138002064929787753525 7\\ 3618605887713749028183 5\end{array}} \bmod p$$

Corollary I: $g^i = g^{i \bmod |H|}$

$$Z \leftarrow g^{\begin{array}{l}3705764346409644403258417782318102824858084594001093 74\\ 8750648996496347171581 6\end{array} \times \begin{array}{l}29177641728484883278069152197089138002064929787753525 7\\ 3618605887713749028183 5\end{array}} \bmod p$$

Computing in groups – exponentiation

Goal: compute $g^n \in G$

Naïve approach: $g^n = \overbrace{g \circ g \circ g \circ \cdots \circ g}^{n}$

- Running time: $n \approx 2^k \implies 2^k$ group operations!
- Doesn't work for exponent sizes used in cryptography

Computing in groups – exponentiation; square-and-multiply

Goal: compute $g^n \in G$

$$n = (b_5 b_4 b_3 b_2 b_1 b_0)_2$$
$$= 2^5 b_5 + 2^4 b_4 + 2^3 b_3 + 2^2 b_2 + 2^1 b_1 + 2^0 b_0$$

$$y_6 \leftarrow e$$
$$y_5 \leftarrow y_6^2 \circ g^{b_5} \quad = g^{b_5}$$
$$y_4 \leftarrow y_5^2 \circ g^{b_4} \quad = g^{2b_5 + b_4}$$
$$y_3 \leftarrow y_4^2 \circ g^{b_3} \quad = g^{2^2 b_5 + 2b_4 + b_3}$$
$$y_2 \leftarrow y_3^2 \circ g^{b_2} \quad = g^{2^3 b_5 + 2^2 b_4 + 2b_3 + b_2}$$
$$y_1 \leftarrow y_2^2 \circ g^{b_1} \quad = g^{2^4 b_5 + 2^3 b_4 + 2^2 b_3 + 2b_2 + b_1}$$
$$y_0 \leftarrow y_1^2 \circ g^{b_0} \quad = g^{2^5 b_5 + 2^4 b_4 + 2^3 b_3 + 2^2 b_2 + 2b_1 + b_0}$$

$$43 = 101011_2$$
$$= 2^5 + 2^3 + 2^1 + 2^0$$

$$y_6 \leftarrow e$$
$$y_5 \leftarrow y_6^2 \circ g^1 \quad = g^1$$
$$y_4 \leftarrow y_5^2 \circ g^0 \quad = g^2$$
$$y_3 \leftarrow y_4^2 \circ g^1 \quad = g^{4+1} = g^5$$
$$y_2 \leftarrow y_3^2 \circ g^0 \quad = g^{10}$$
$$y_1 \leftarrow y_2^2 \circ g^1 \quad = g^{20+1} = g^{21}$$
$$y_0 \leftarrow y_1^2 \circ g^1 \quad = g^{42+1} = g^{43}$$

Computing in groups – exponentiation; square-and-multiply

Goal: compute $g^n \in G$

$$n = (b_5 b_4 b_3 b_2 b_1 b_0)_2$$
$$= 2^5 b_5 + 2^4 b_4 + 2^3 b_3 + 2^2 b_2 + 2^1 b_1 + 2^0 b_0$$

$$43 = 101011_2$$
$$= 2^5 + 2^3 + 2^1 + 2^0$$

$y_6 \leftarrow e$

$y_5 \leftarrow y_6^2 \circ g^{b_5} \quad = g^{b_5}$

$y_4 \leftarrow y_5^2 \circ g^{b_4} \quad = g^{2b_5 + b_4}$

$y_3 \leftarrow y_4^2 \circ g^{b_3} \quad = g^{2^2 b_5 + 2b_4 + b_3}$

$y_2 \leftarrow y_3^2 \circ g^{b_2} \quad = g^{2^3 b_5 + 2^2 b_4 + 2b_3 + b_2}$

$y_1 \leftarrow y_2^2 \circ g^{b_1} \quad = g^{2^4 b_5 + 2^3 b_4 + 2^2 b_3 + 2b_2 + b_1}$

$y_0 \leftarrow y_1^2 \circ g^{b_0} \quad = g^{2^5 b_5 + 2^4 b_4 + 2^3 b_3 + 2^2 b_2 + 2b_1 + b_0}$

Square–and–Multiply$(g \in G, n \in \boldsymbol{Z})$

1. **if** $n < 0$ **then** $g \leftarrow g^{-1}$ and $n \leftarrow |n|$
2. $n = (b_{t-1} \ldots b_1 b_0)_2$
3. $y \leftarrow e$
4. **for** $i = t - 1$ **downto** 0 **do**
5. $\quad y \leftarrow y^2 \circ g^{b_i}$
6.
7. **return** y

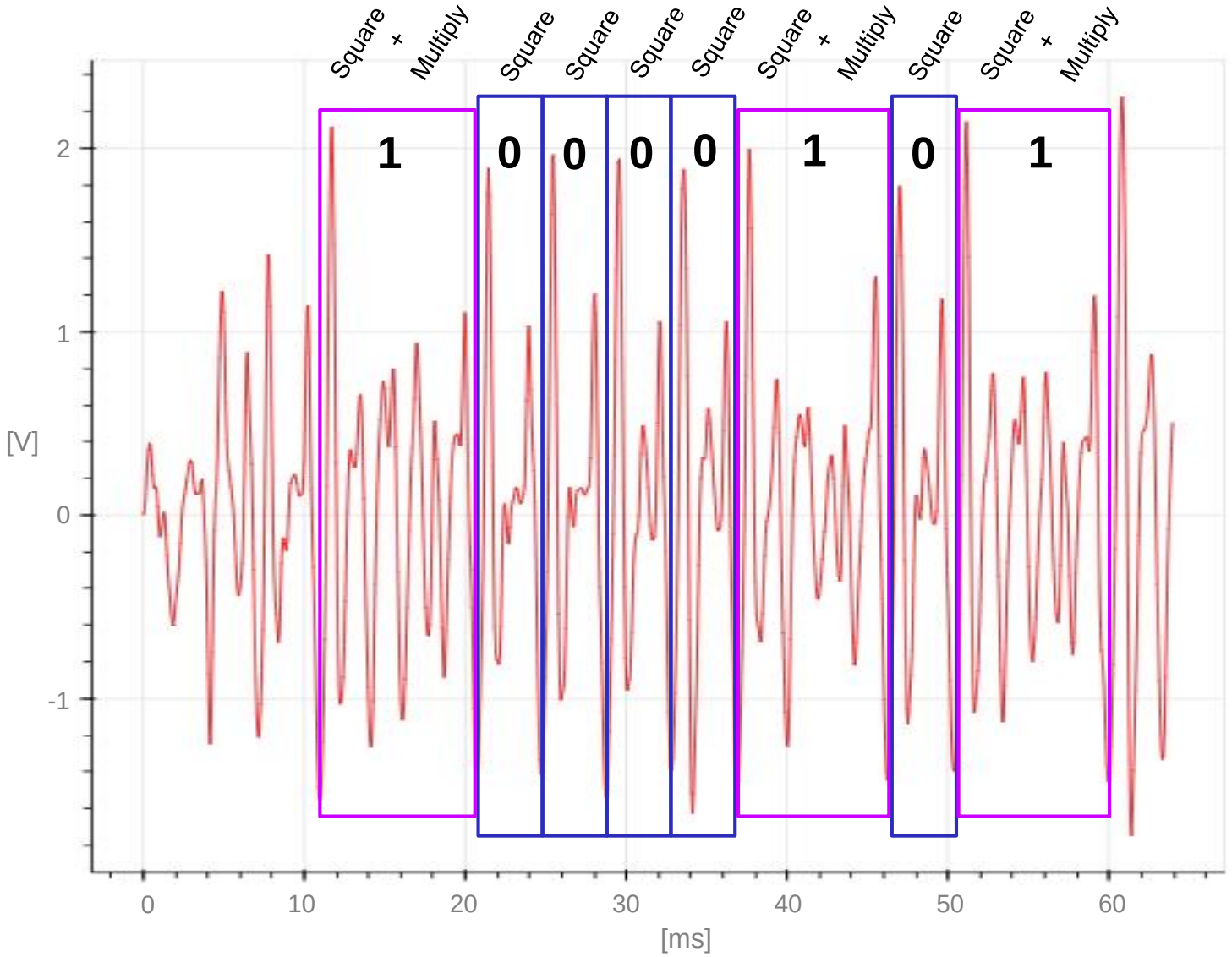
Square-and-multiply

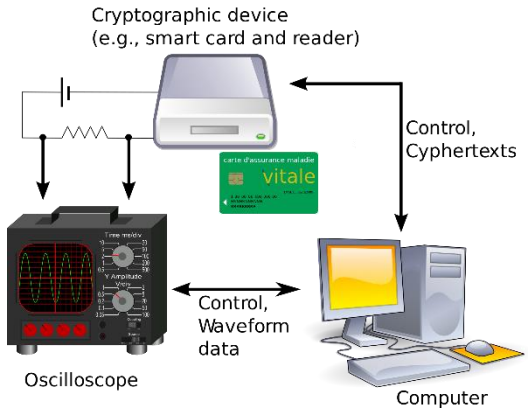
- $\left(\boldsymbol{Z}_p^*, \cdot\right)$
  - Naïve exponentiation: $\mathcal{O}(n) \approx p$
  - Square-and-multiply: $\mathcal{O}(t) = \mathcal{O}(\log_2 n) \approx \log_2 p$
  - $\approx 2^{2048}$ vs. ≈ 2048 multiplications for $p \approx 2^{2048}$

- Prime-order subgroup $H < \left(\boldsymbol{Z}_p^*, \cdot\right)$
  - Naïve exponentiation: $\mathcal{O}(n) \approx q$
  - Square-and-multiply: $\mathcal{O}(t) = \mathcal{O}(\log_2 n) \approx \log_2 q$
  - $\approx 2^{256}$ vs. ≈ 256 multiplications for $q \approx 2^{256}$ and $p \approx 2^{2048}$

- $\left(E\left(\boldsymbol{F}_p\right), +\right)$
  - Naïve "exponentiation" (i.e., point multiplication nP): $\mathcal{O}(n) \approx \left|E\left(\boldsymbol{F}_p\right)\right|$
  - "Square-and-multiply" (i.e., double-and-add): $\mathcal{O}(t) = \mathcal{O}(\log_2 n) \approx \log_2\left|E\left(\boldsymbol{F}_p\right)\right|$
  - $\approx 2^{256}$ vs. ≈ 256 elliptic-curve additions for NIST P-256 or Curve25519

Side-channel attacks – power analysis



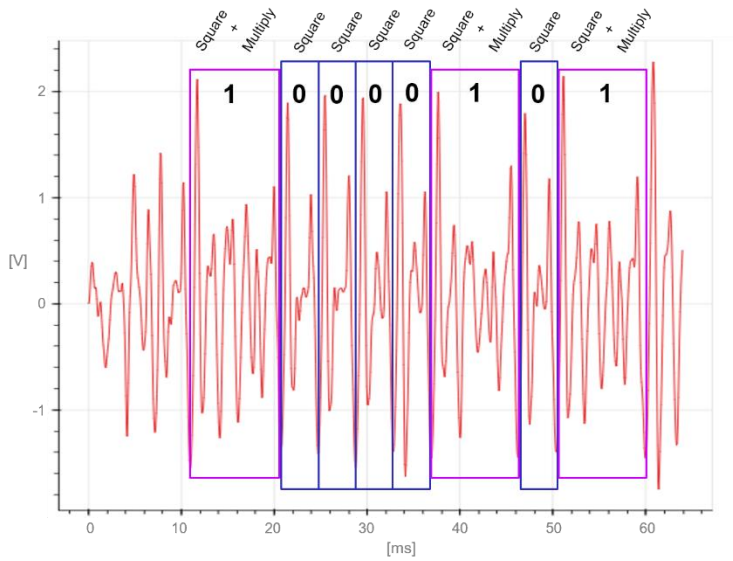


Square–and–Multiply$(g \in G\,, n \in \boldsymbol{Z})$

1. **if** $n < 0$ **then** $g \leftarrow g^{-1}$ and $n \leftarrow |n|$
2. $n = (b_{t-1} \ldots b_1 b_0)_2$
3. $y \leftarrow e$
4. **for** $i = t - 1$ **downto** 0 **do**
5. $\quad y \leftarrow y^2$
6. $\quad$ **if** $b_i = 1$ **then**
7. $\quad\quad y \leftarrow y \circ g$
8. **return** y

Mitigations

- Power (and time) difference between $b_i = 0$ and $b_i = 1$



- Solution: Square-and-*Always*-Multiply

Square–and–always–Multiply$(g \in G, n \in \boldsymbol{Z})$

1. **if** $n < 0$ **then** $g \leftarrow g^{-1}$ and $n \leftarrow |n|$
2. $n = (b_{t-1} \dots b_1 b_0)_2$
3. $y \leftarrow e$
4. **for** $i = t - 1$ **downto** 0 **do**
5. $\quad y \leftarrow y^2$
6. $\quad z \leftarrow y \circ g$ // always perform multiplication
7. $\quad$ **if** $b_i = 1$ **then**
8. $\quad\quad y \leftarrow z$
9. **return** y

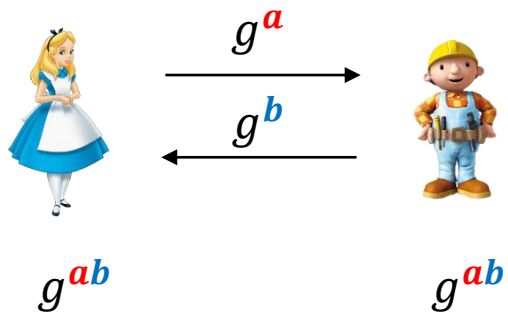
- Wastes computations: $\approx t/2$ of multiplications thrown away
- Better solutions: Montgomery ladders

Square–and–Multiply$(g \in G, n \in \boldsymbol{Z})$

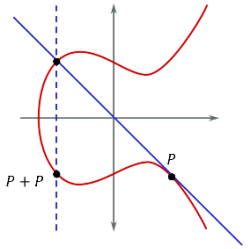
1. **if** $n < 0$ **then** $g \leftarrow g^{-1}$ and $n \leftarrow |n|$
2. $n = (b_{t-1} \dots b_1 b_0)_2$
3. $y \leftarrow e$
4. **for** $i = t - 1$ **downto** 0 **do**
5. $\quad y \leftarrow y^2$
6. $\quad$ **if** $b_i = 1$ **then**
7. $\quad\quad y \leftarrow y \circ g$
8. **return** y

Diffie-Hellman – computations

- $\left(\boldsymbol{Z}_p^*, \cdot\right)$
  - Find prime p (one-time)
  - Find generator $\langle g \rangle = \left(\boldsymbol{Z}_p^*, \cdot\right)$ (one-time)
  - Compute $g^a = gg \cdots g \mod p$
    - Multiply $x \cdot y \mod p$



- $\left(E\left(\boldsymbol{F}_p\right), +\right)$
  - Find prime p (one-time)
  - Generate curve $y^2 = x^3 + ax + b \mod p$ (one-time)
  - Find curve group order $\left|E\left(\boldsymbol{F}_p\right)\right|$ (one-time)
  - Find generator P (one-time)
  - Compute $aP = P + P + \cdots + P$
    - Point addition



Finding prime numbers

- We need *large* prime numbers
  - Both for $(\boldsymbol{Z}_p^*, \cdot)$ and $(E(\boldsymbol{F}_p), +)$
- No efficient "prime-generating" formula is known
- Simple idea: pick random number and check if it's prime
- Efficient? $\Longrightarrow$ What is the success probability?
  - Depends on the ratio primes / non-primes
  - $\pi(n) =$ "#prime numbers $\leq n$"
  - **Prime Number Theorem:** $\frac{\pi(n)}{n} \approx \frac{1}{\ln n}$
  - 2048-bit number: ≈ 700 trials needed

GenPrime(k)

1. **while** true **do**
2. $\quad n \xleftarrow{\$}$ odd k-bit integer
3. $\quad$ **if** IsPrime$(n) =$ PRIME **then**
4. $\quad\quad$ **return** n

$$n \approx 2^{2048} \Longrightarrow \frac{\pi(n)}{n} \approx \frac{1}{\ln 2^{2048}} \approx \frac{1}{1400}$$

n	100	1000	10^6	10^9	10^{12}	10^{15}
$\pi(n)$	25	168	$\approx 78 \cdot 10^3$	$\approx 50 \cdot 10^6$	$\approx 30 \cdot 10^9$	$\approx 29 \cdot 10^{12}$

Finding prime numbers

- We need *large* prime numbers
  - Both for $(\boldsymbol{Z}_p^*, \cdot)$ and $(E(\boldsymbol{F}_p), +)$

- Naïve $\mathrm{IsPrime}(n)$:
  - 3 divides n? Not prime
  - 5 divides n? Not prime
  - 7 divides n? Not prime
  - ⋮
  - $\lfloor \sqrt{n} \rfloor$ divides n? Not prime
  - n is prime!

  - *Very* inefficient: $n \approx 2^k \implies \pi(n) \approx \frac{2^k}{\ln 2^k} \approx \frac{2^k}{k}$

- Want: a simple property which *only* holds for prime numbers

GenPrime(k)

1. **while** true **do**
2. $n \xleftarrow{\$}$ odd k-bit integer
3. **if** $\mathrm{IsPrime}(n) = \mathrm{PRIME}$ **then**
4. **return** n

Fermat's theorem

Theorem: if $(G,\circ)$ is a finite group, then for all $g \in G$:

$$g^{|G|} = e$$

$\left(\boldsymbol{Z}_p^*,\cdot\right) = \{1,2,\ldots,p-1\}$ under multiplication modulo p $\quad \left|\boldsymbol{Z}_p^*\right| = p-1 \quad e = 1$

Fermat's theorem: if p is prime, then for all $a \not\equiv 0 \pmod p$:

$$a^{p-1} \equiv 1 \pmod p$$

$$2^{560} = 1 \bmod 561$$
$$3^{560} = 1 \bmod 561$$
$$4^{560} = 1 \bmod 561$$
$$\vdots$$
$$560^{560} = 1 \bmod 561$$

$A \quad \not\Longleftarrow \quad B$

p is prime $\Longrightarrow$ *all* $a \not\equiv 0 \bmod p$ satisfy Fermat's theorem

p is **not** prime $\Longleftarrow$ *some* $a \not\equiv 0 \bmod p$ does **not** satisfy Fermat's theorem

$\bar{A} \qquad\qquad \bar{B}$

Carmichael number

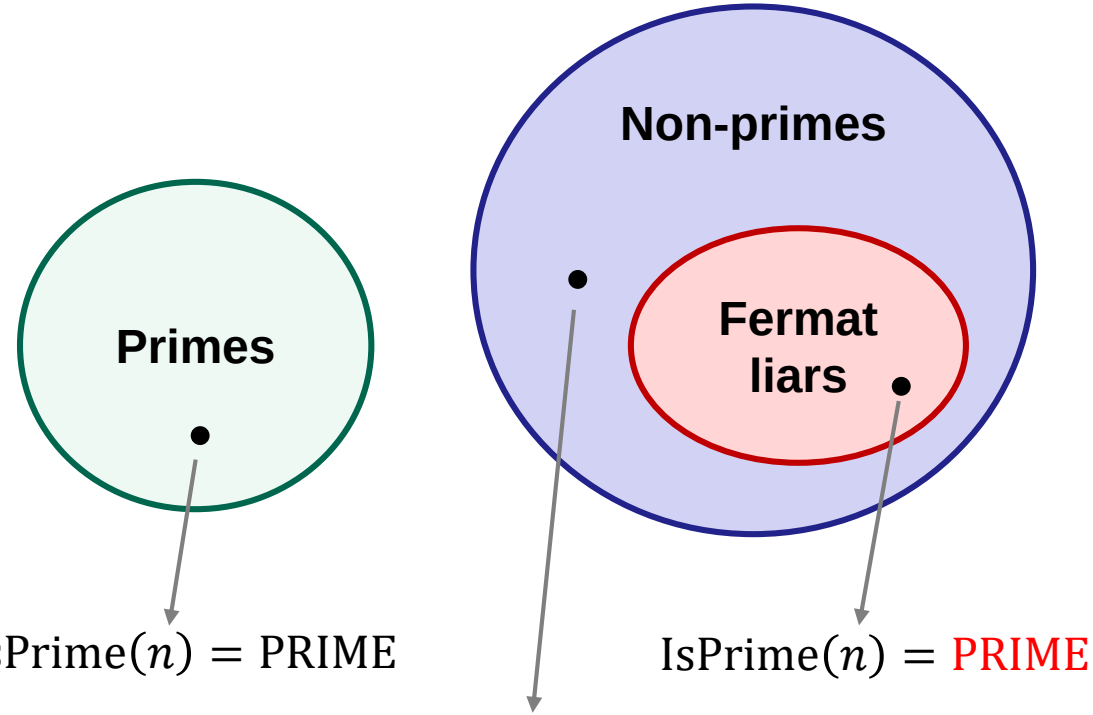
Fermat primality test

Fermat's theorem: if p is prime, then for all $a \neq 0 \pmod p$:

$$a^{p-1} \equiv 1 \pmod p$$

IsPrime(n)

1. **for** $a \in \{2, 3, \ldots, t\}$ **do**
2. **if** $a^{n-1} \neq 1 \mod n$ **then**
3. **return** NOT-PRIME
4. **return** PRIME



Better tests exist:

- Euler-test (Solovay-Strassen algorithm)
- Strong pseudoprime-test (Miller-Rabin algorithm)

Finding primes

IsPrime(n) // Fermat

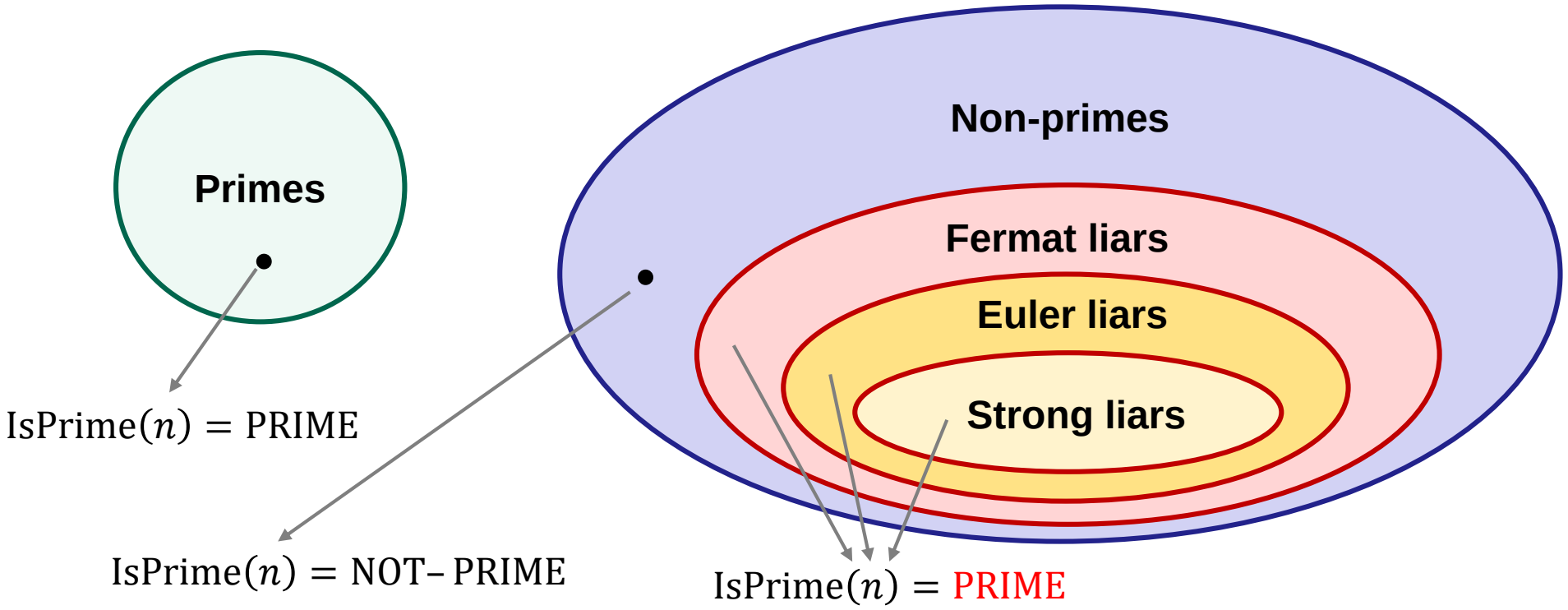
```
1.  for a ∈ {2, 3, … , t} do
2.      if ¬FermatTest(a, n) then
3.          return NOT-PRIME
4.  return PRIME
```

IsPrime(n) // Solovay-Strassen

```
1.  for a ∈ {2, 3, … , t} do
2.      if ¬EulerTest(a, n) then
3.          return NOT-PRIME
4.  return PRIME
```

IsPrime(n) // Miller-Rabin

```
1.  for a ∈ {2, 3, … , t} do
2.      if ¬StrongTest(a, n) then
3.          return NOT-PRIME
4.  return PRIME
```



Finding primes in practice

- Miller-Rabin most used in practice
- Failure probability $\leq \frac{1}{4^t}$

IsPrime(n) // Miller-Rabin

```
1.  for a ∈ {2, 3, ..., t} do
2.      if ¬StrongTest(a, n) then
3.          return NOT-PRIME
4.  return PRIME
```

- *Deterministic* primality tests
  - Many existed…but none running in polynomial time (P)
  - Open problem for a long time
  - *Agrawal, Kayal & Saxena '02*: "PRIMES is in P"
  - Original running time $\approx \mathcal{O}(k^{12})$
  - Quickly improved to $\approx \mathcal{O}(k^6)$

Finding generators

- Easy in prime-order groups
  - All non-identity elements are generators!

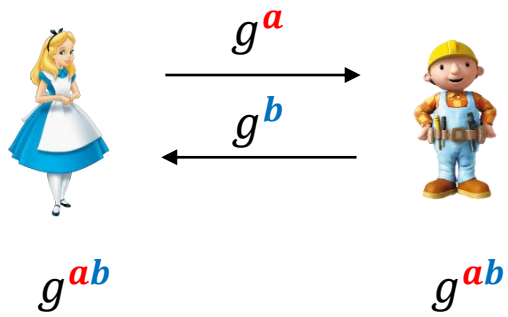
Corollary II (Lagrange's theorem):

if $H < G$ then $|H|$ divides $|G|$

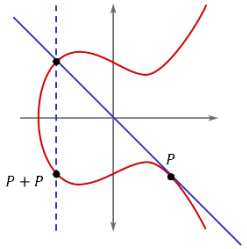
- $\left(\boldsymbol{Z}_p^*, \cdot\right)$
  - Not prime-order!
  - Common in practice: pick element at random; check if generator

Diffie-Hellman – computations

- $\left(\boldsymbol{Z}_p^*, \cdot\right)$
  - Find prime p (one-time)
  - Find generator $\langle g \rangle = \left(\boldsymbol{Z}_p^*, \cdot\right)$ (one-time)
  - Compute $g^a = gg \cdots g \mod p$
    - Multiply $x \cdot y \mod p$



- $\left(E\left(\boldsymbol{F}_p\right), +\right)$
  - Find prime p (one-time)
  - Generate curve $y^2 = x^3 + ax + b \mod p$ (one-time)
  - Find curve group order $\left|E\left(\boldsymbol{F}_p\right)\right|$ (one-time)
  - Find generator P (one-time)
  - Compute $aP = P + P + \cdots + P$
    - Point addition



Schoof's algorithm

Tricky!

$\left|E\left(\boldsymbol{F}_p\right)\right| \neq p$ (typically)

Easy ($\left|E\left(\boldsymbol{F}_p\right)\right|$ is usually prime)

Diffie-Hellman – man-in-the-middle attack

$$G = \langle g \rangle$$

$$A = g^a$$

$$B = g^b$$

$$a \xleftarrow{\$} \{1, \dots, |G|\}$$

$$b \xleftarrow{\$} \{1, \dots, |G|\}$$

$$Z \leftarrow B^a = g^{ab}$$

$$Z \leftarrow A^b = g^{ab}$$

Diffie-Hellman – man-in-the-middle attack

$G = \langle g \rangle$

$A = g^a$

$X = g^x$

$B = g^b$

$a \xleftarrow{\$} \{1, \ldots, |G|\}$

$b \xleftarrow{\$} \{1, \ldots, |G|\}$

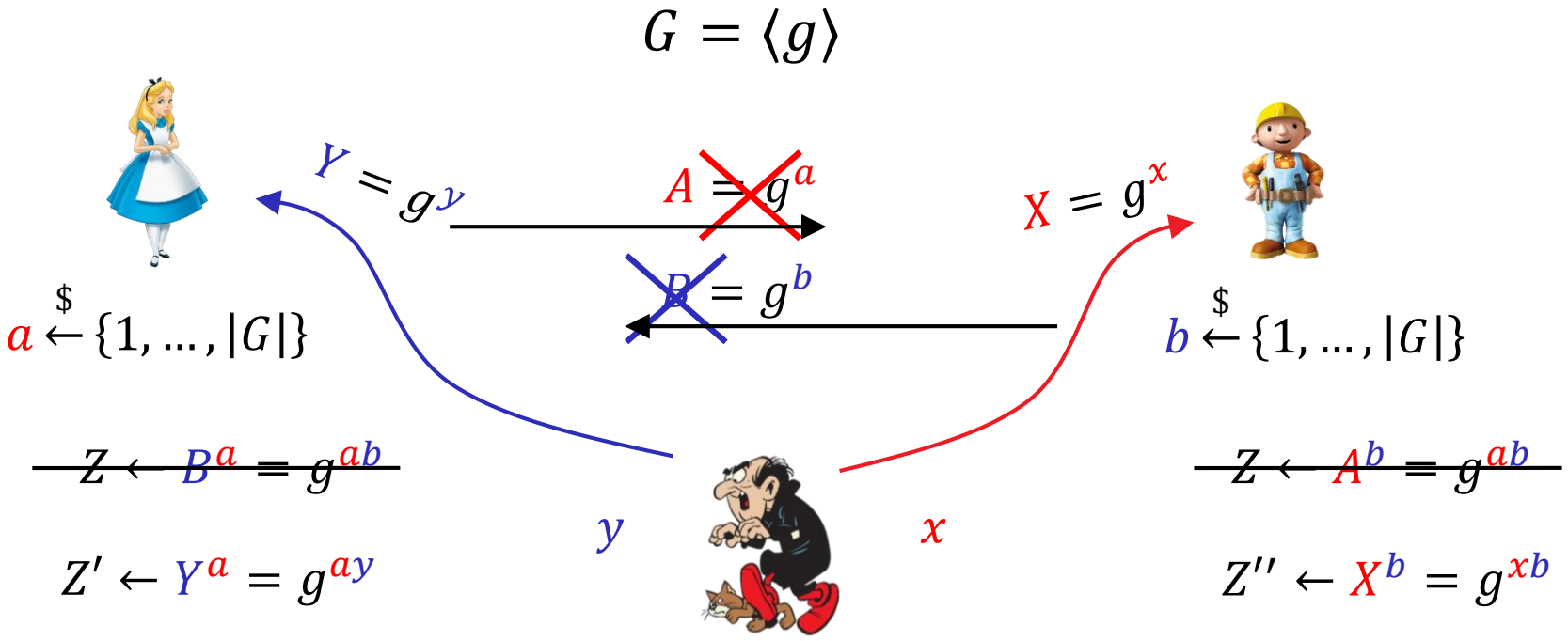
$Z \leftarrow B^a = g^{ab}$

x

~~$Z \leftarrow A^b = g^{ab}$~~

$Z'' \leftarrow X^b = g^{xb}$

Diffie-Hellman – man-in-the-middle attack



Noise-protocol

Long-term key

$A = g^a$

$G = \langle g \rangle, A, B$

$B = g^b$

Long-term key

$X = g^x$

$Y = g^y$

$x \xleftarrow{\$} \{1, \dots, |G|\}$

$y \xleftarrow{\$} \{1, \dots, |G|\}$

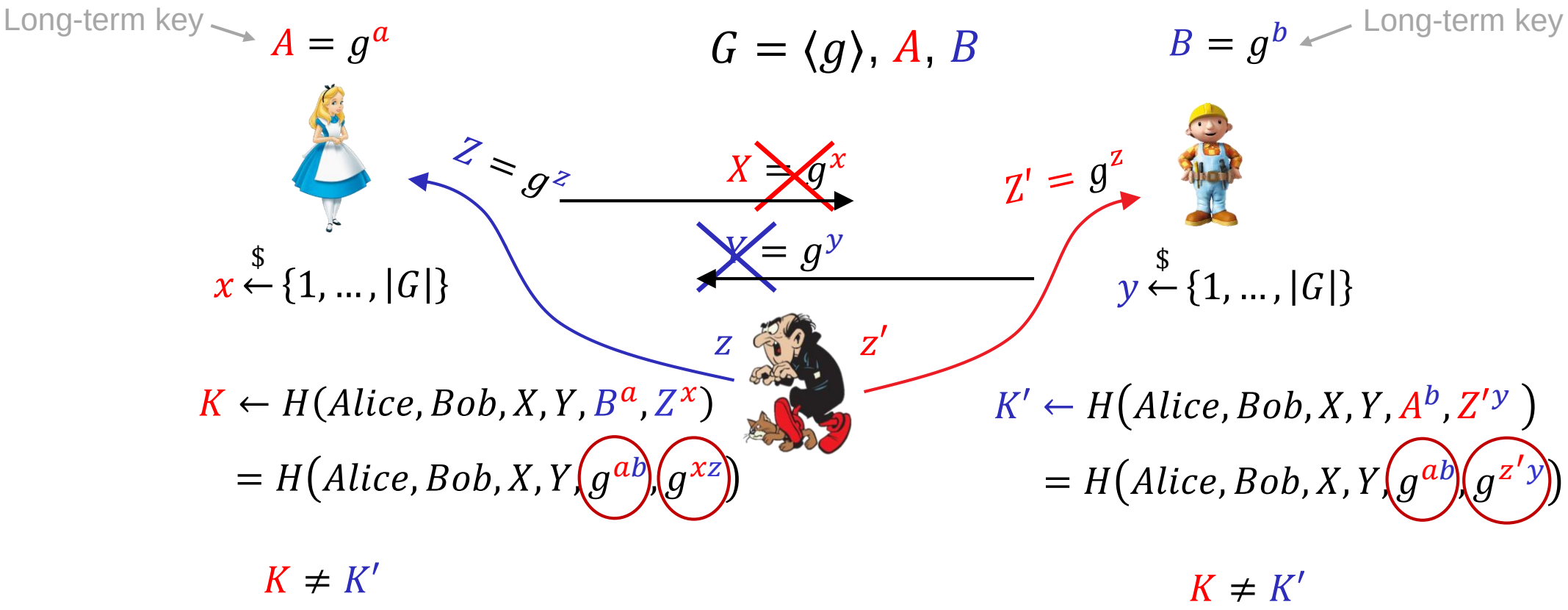
$K \leftarrow H(Alice, Bob, X, Y, B^a, Y^x)$

$= H(Alice, Bob, X, Y, g^{ab}, g^{xy})$

$K \leftarrow H(Alice, Bob, X, Y, A^b, X^y)$

$= H(Alice, Bob, X, Y, g^{ab}, g^{xy})$

Noise-protocol



Can't compute K or K'!

Noise-protocol

Long-term key → $A = g^a$

$G = \langle g \rangle, A, B$

$B = g^b$ ← Long-term key

$X = g^x$ →

← $Y = g^y$

$x \xleftarrow{\$} \{1, \dots, |G|\}$

$y \xleftarrow{\$} \{1, \dots, |G|\}$

$$K \leftarrow H(Alice, Bob, X, Y, B^a, Y^x)$$
$$= H(Alice, Bob, X, Y, g^{ab}, g^{xy})$$

$$K \leftarrow H(Alice, Bob, X, Y, A^b, X^y)$$
$$= H(Alice, Bob, X, Y, g^{ab}, g^{xy})$$

Many alternatives:

$K \leftarrow H(Alice, Bob, X, Y, g^{ay}, g^{xb})$ static-ephemeral, ephemeral-static

$K \leftarrow H(Alice, Bob, X, Y, g^{ay}, g^{xb}, g^{xy})$ static-ephemeral, ephemeral-static, ephemeral-ephemeral

$K \leftarrow H(Alice, Bob, X, Y, g^{ab}, g^{ay}, g^{xb}, g^{xy})$ static-static, ephemeral-static, ephemeral-ephemeral, ephemeral-ephemeral

Summary

- Special algorithms needed to deal with the large numbers in asymmetric cryptography
  - Square-and-multiply for group exponentiation
    - Not secure against side-channel attacks
  - Prime finding
    - Common in practice: pick random number; check if prime
    - Primality tests: Fermat's, Miller-Rabin (small one-sided error)

- Plain Diffie-Hellman is *not* secure against active adversaries
  - Man-in-the-middle attack
  - Problem: lack of authentication
  - Common solution: digital signatures (used in TLS, IPsec, SSH)
  - Modern solution: long-term Diffie-Hellman keys mixed with ephemeral Diffie-Hellman keys
    - Noise protocol, Signal, What'sApp, Facebook Messenger Secret Conversations