Vorkurs für Studierende in Mathematik und Physik
Einführung in Kryptographie

Felix Fontein

Institut für Mathematik
Universität Zürich

14. September 2018

Kryptologie

- Kryptographie: Konzeption und Konstruktion von Systemen, die Informationen absichern
- Kryptoanalyse: solche Systeme untersuchen, um ihre Sicherheit nachzuweisen oder um sie zu brechen

Heute: Kryptographie

Zwei Hauptthemen der Kryptographie:

- das sichere Austauschen von (geheime) Informationen
- das «Unterschreiben» (Signieren) von Nachrichten

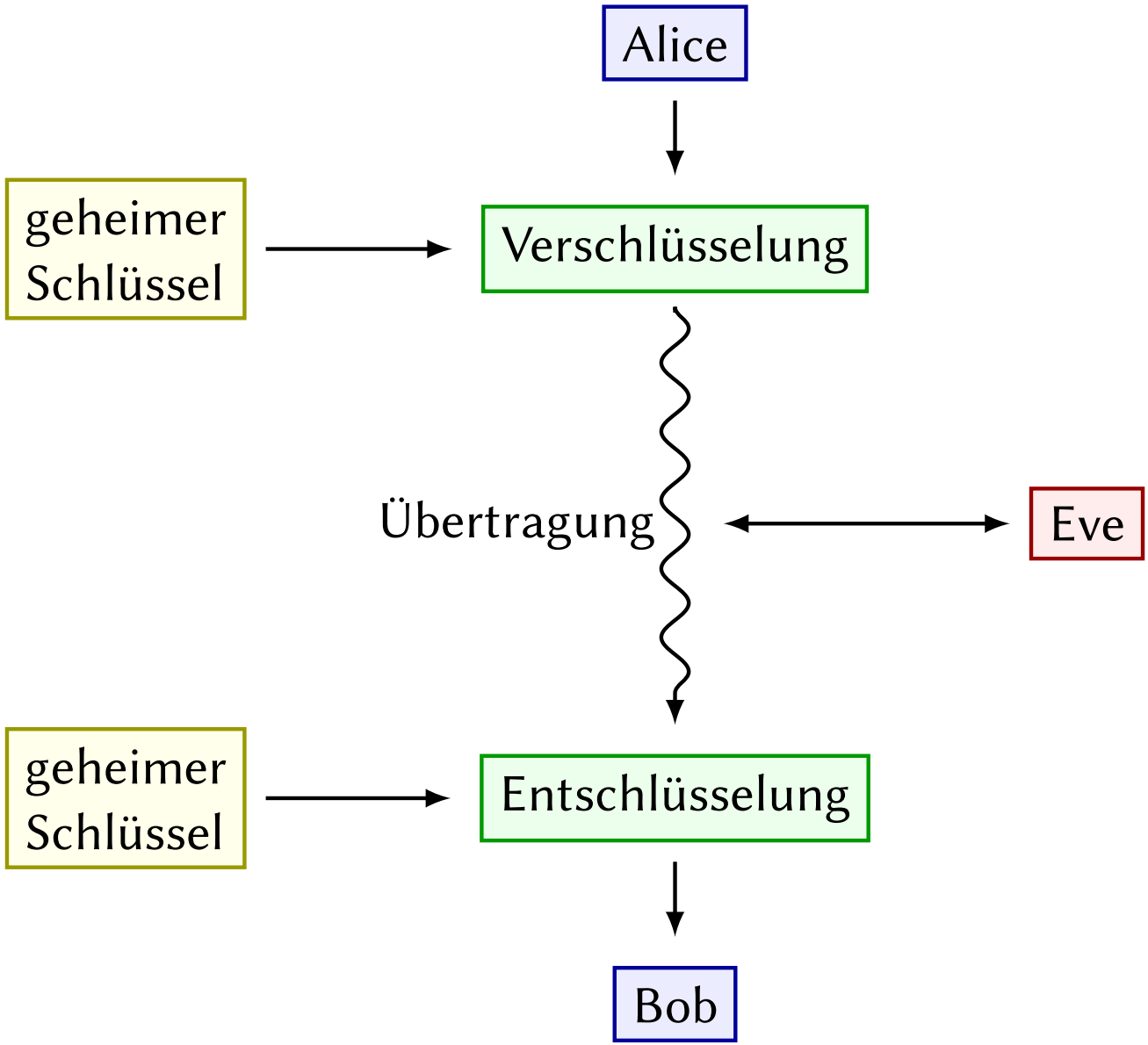
Heute: Kryptographie

Zwei Hauptthemen der Kryptographie:

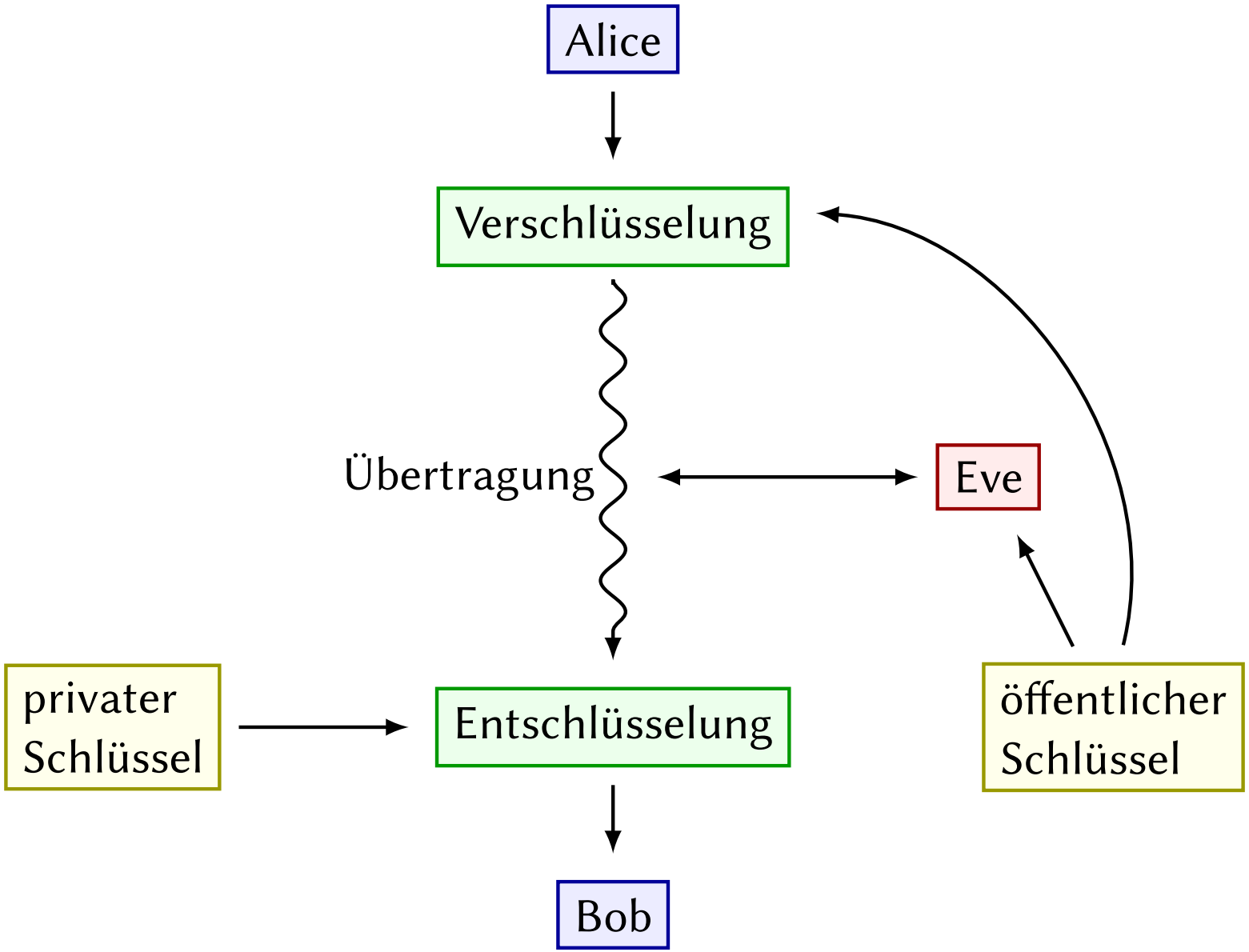
- das sichere Austauschen von (geheime) Informationen
- das «Unterschreiben» (Signieren) von Nachrichten

Heute: nur erster Punkt

Symmetrische Kryptographie (Secret Key)



Asymmetrische Kryptographie (Public Key)



Asymmetrische Kryptographie (Public Key)

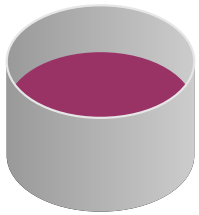
- 1976: Diffie-Hellman-Schlüsselaustausch (W. Diffie, M. Hellman)
- 1977: RSA (R. Rivest, Shamir, Adleman)
- 1985: N. Koblitz und V. Miller schlagen elliptische Kurven vor

Asymmetrische Kryptographie (Public Key)

- 1976: Diffie-Hellman-Schlüsselaustausch (W. Diffie, M. Hellman)
- 1977: RSA (R. Rivest, Shamir, Adleman)
- 1985: N. Koblitz und V. Miller schlagen elliptische Kurven vor

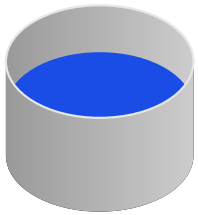
Heute: Diffie-Hellman-Schlüsselaustausch

Diffie-Hellman-Schlüsselaustausch mit Farben

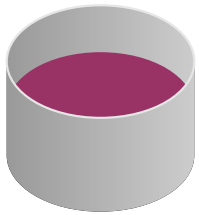


Grundfarbe

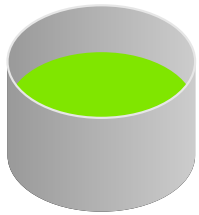
Diffie-Hellman-Schlüsselaustausch mit Farben



Alices geheime Farbe

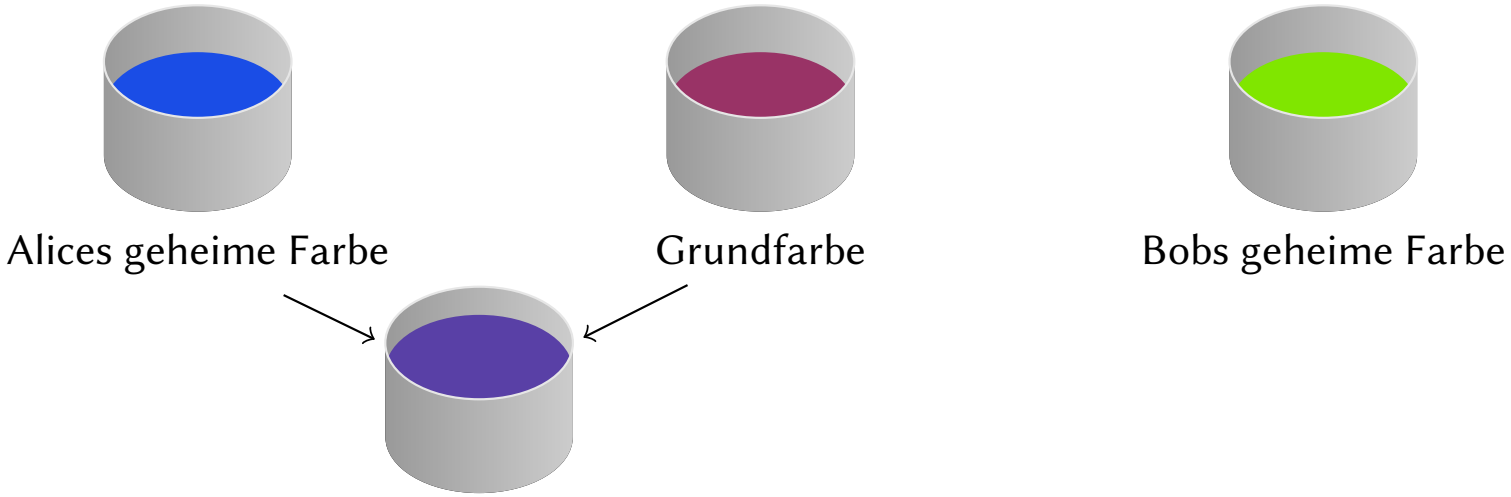


Grundfarbe

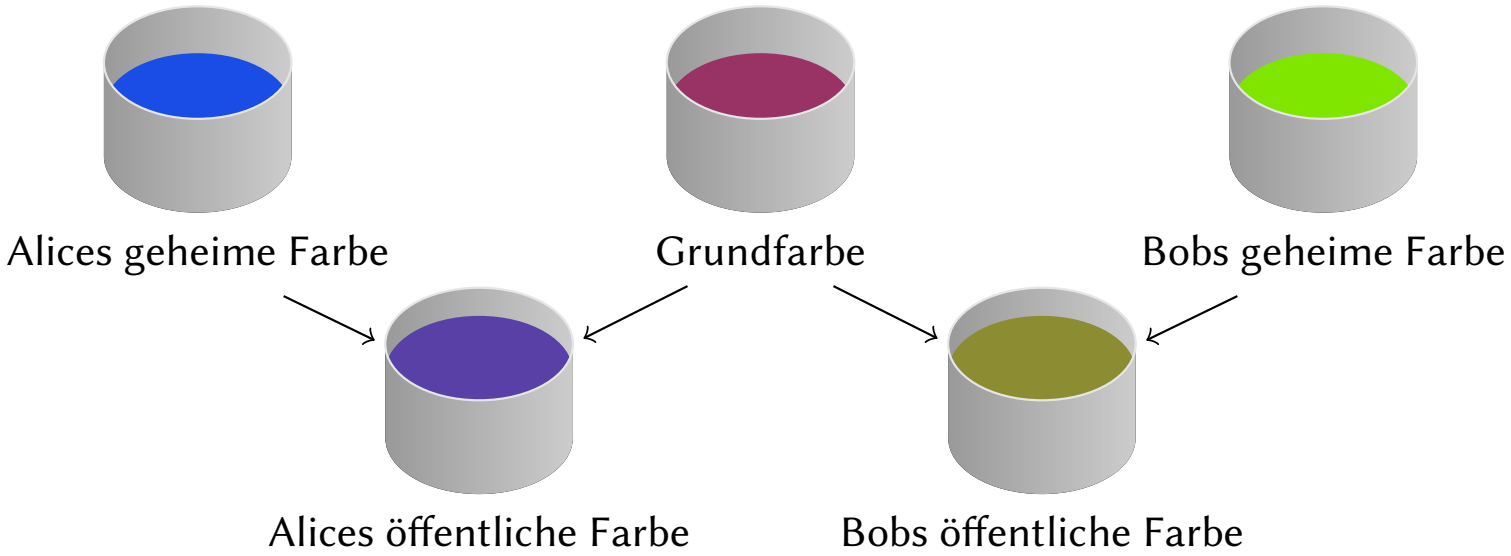


Bobs geheime Farbe

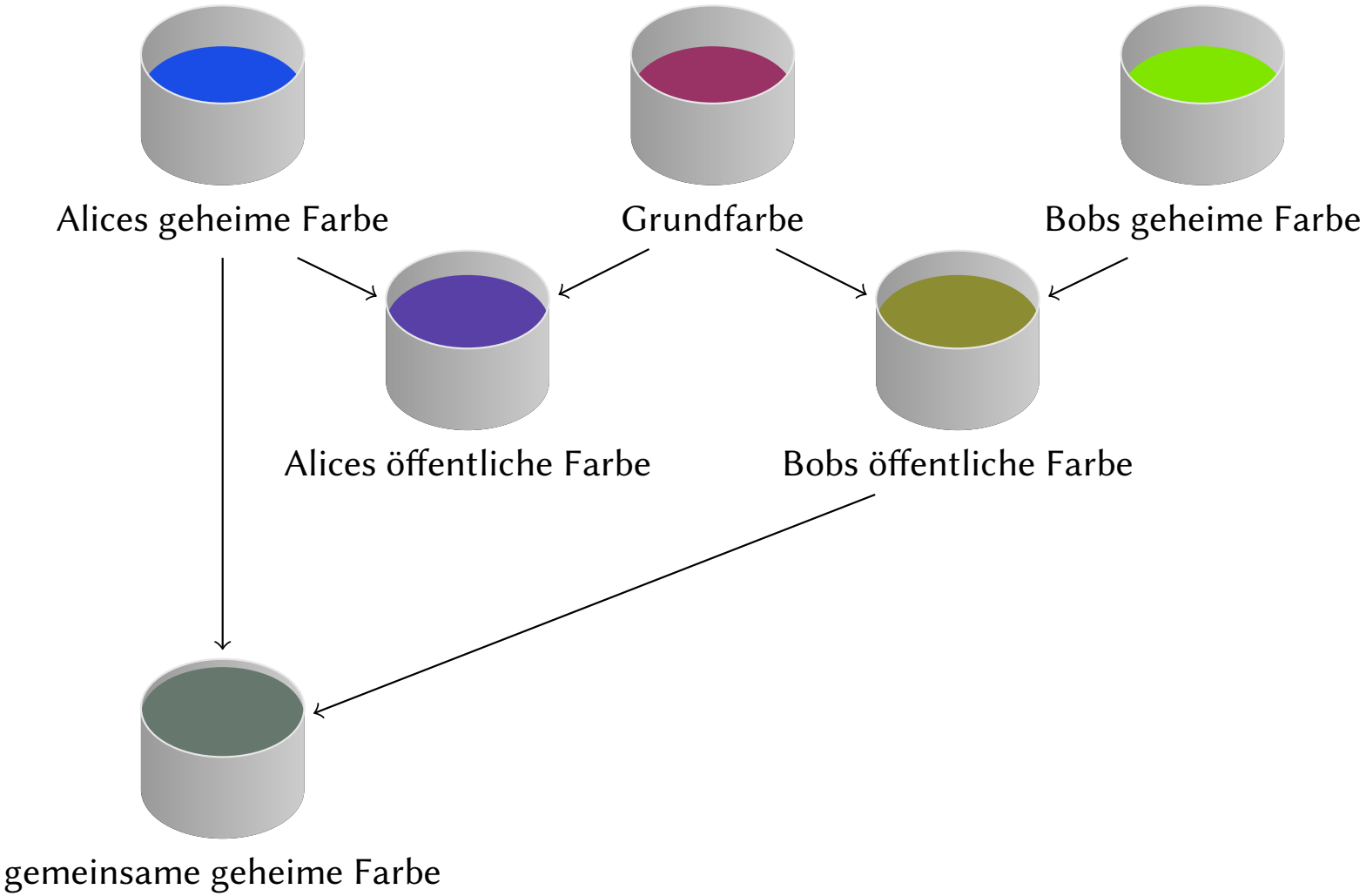
Diffie-Hellman-Schlüsselaustausch mit Farben



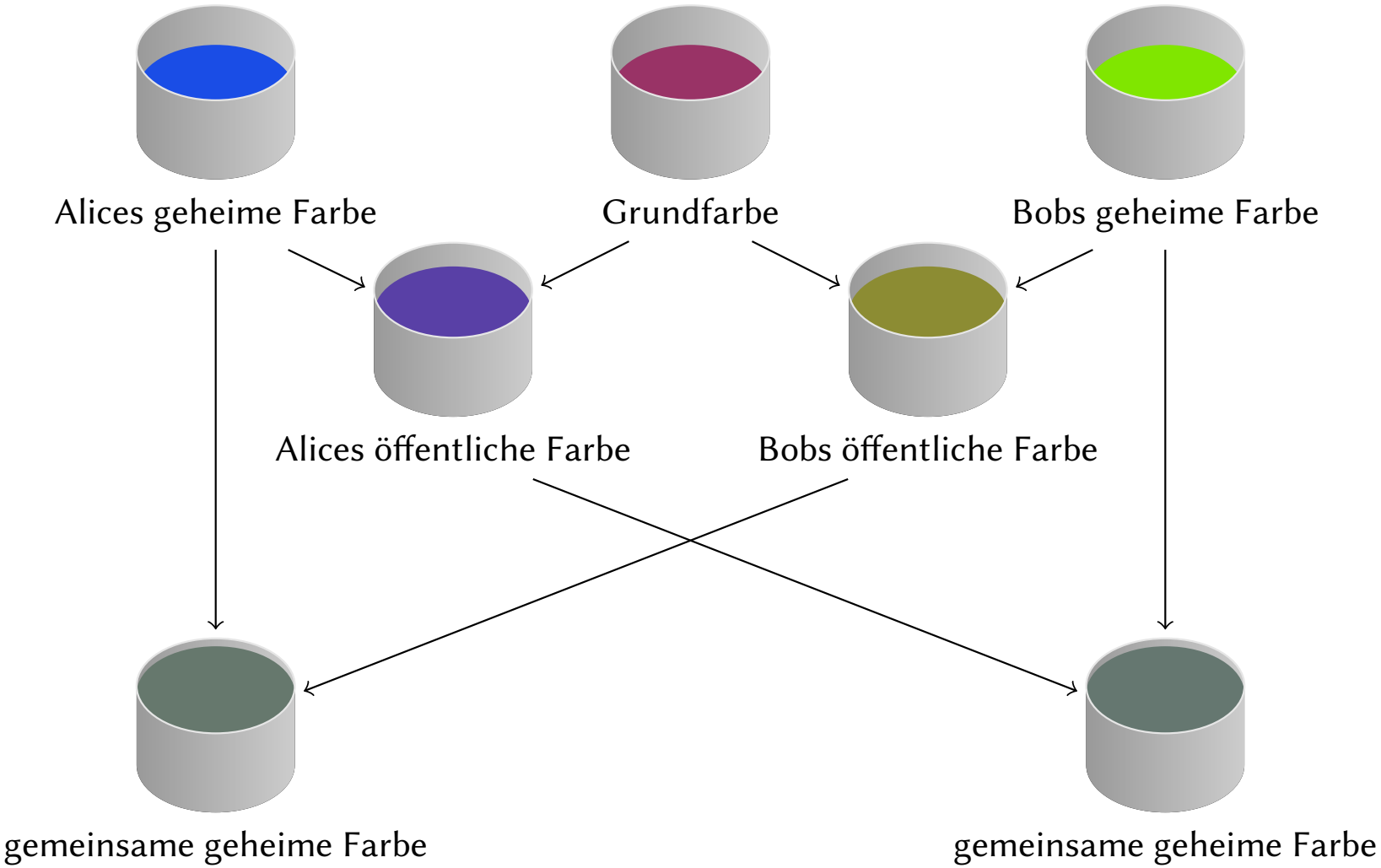
Diffie-Hellman-Schlüsselaustausch mit Farben



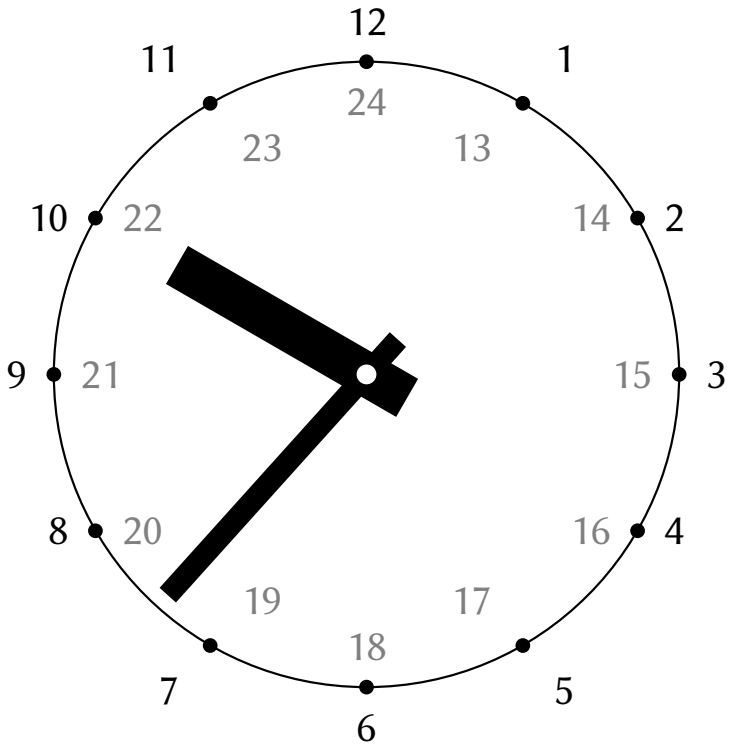
Diffie-Hellman-Schlüsselaustausch mit Farben



Diffie-Hellman-Schlüsselaustausch mit Farben



Modulo-Rechnung



Modulo-Rechnung

Definition

$x \equiv y \pmod{n}$ genau dann, wenn $x - y$ ganzzahliges Vielfaches von n ist.

Modulo-Rechnung

Definition

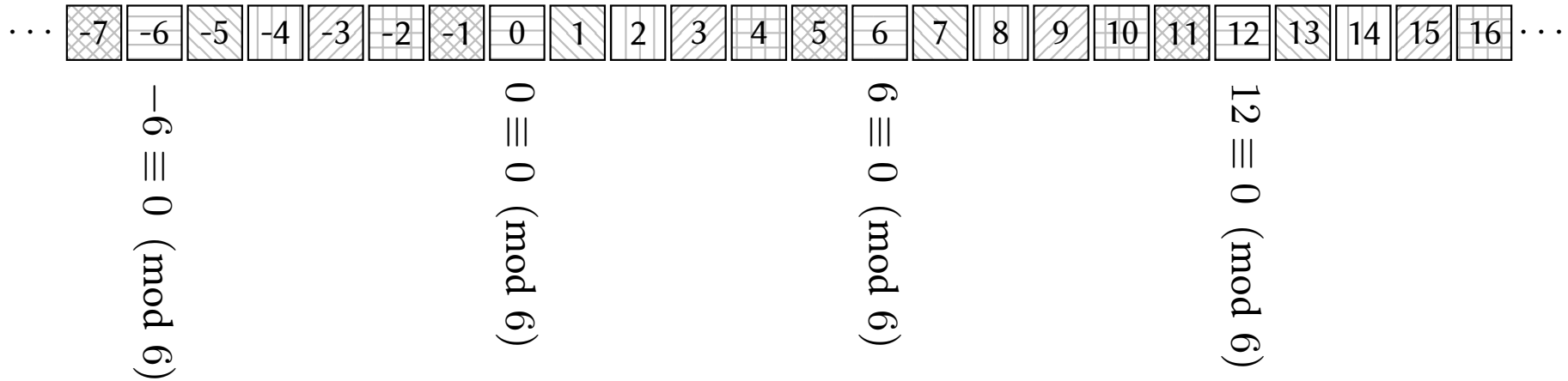
$x \equiv y \pmod{n}$ genau dann, wenn $x - y$ ganzzahliges Vielfaches von n ist.

$\cdots$ | -7 | -6 | -5 | -4 | -3 | -2 | -1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 $\cdots$

Modulo-Rechnung

Definition

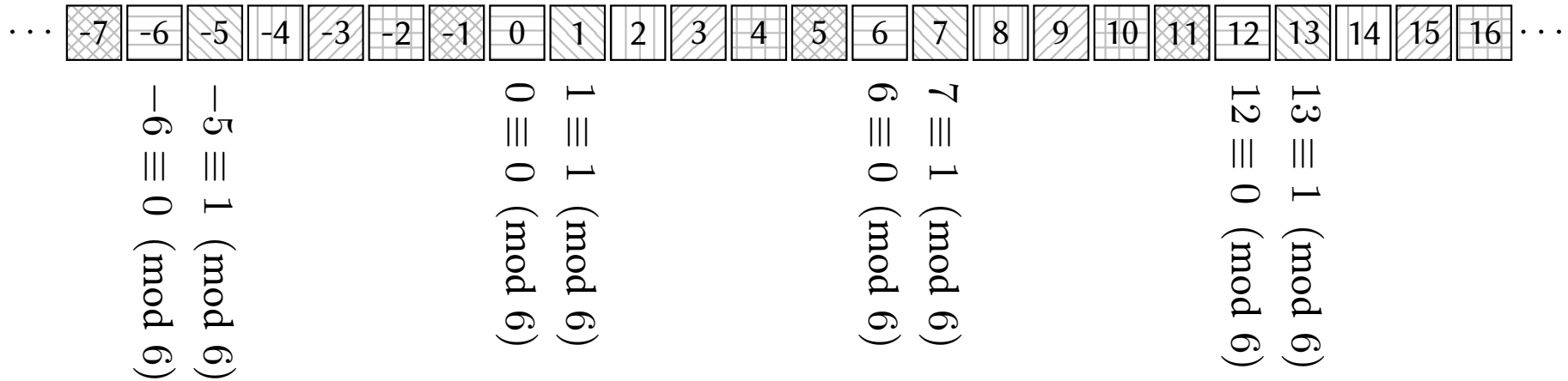
$x \equiv y \pmod{n}$ genau dann, wenn $x - y$ ganzzahliges Vielfaches von n ist.



Modulo-Rechnung

Definition

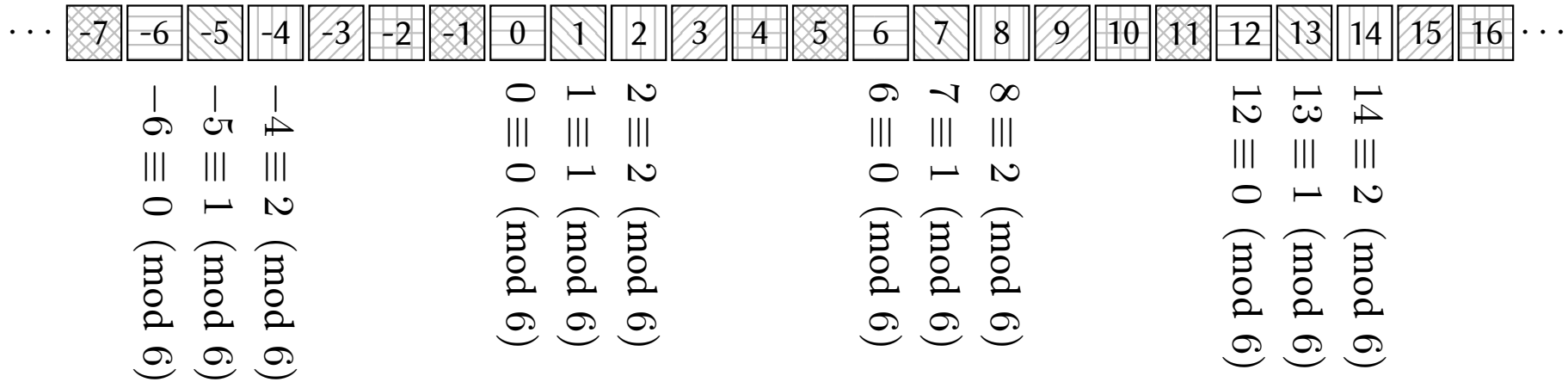
$x \equiv y \pmod{n}$ genau dann, wenn $x - y$ ganzzahliges Vielfaches von n ist.



Modulo-Rechnung

Definition

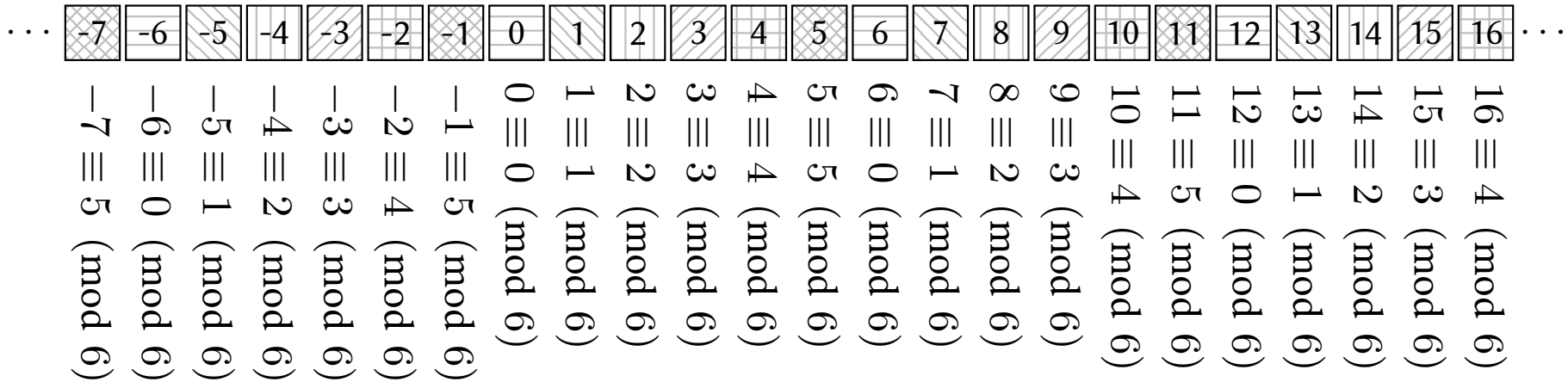
$x \equiv y \pmod{n}$ genau dann, wenn $x - y$ ganzzahliges Vielfaches von n ist.



Modulo-Rechnung

Definition

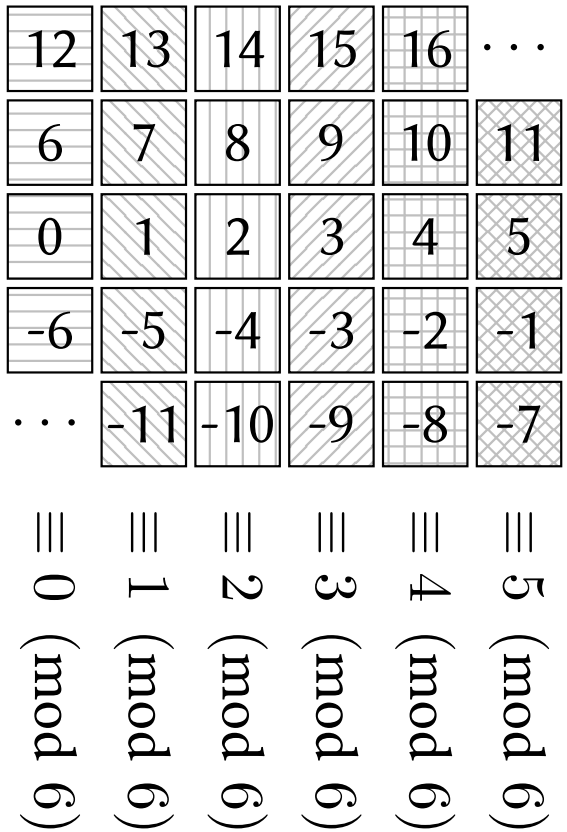
$x \equiv y \pmod{n}$ genau dann, wenn $x - y$ ganzzahliges Vielfaches von n ist.



Modulo-Rechnung

Definition

$x \equiv y \pmod{n}$ genau dann, wenn $x - y$ ganzzahliges Vielfaches von n ist.



Modulo-Rechnung

Definition

$x \equiv y \pmod{n}$ genau dann, wenn $x - y$ ganzzahliges Vielfaches von n ist.

Definition (Restklassen)

Sei $y, n \in \mathbb{Z}$. Dann heisst die Menge $\{x \in \mathbb{Z} \mid x \equiv y \pmod{n}\}$ die Restklasse von y modulo n und wird als $\overline{y}_n$ geschrieben. Die Menge aller Restklassen modulo n, $\{\overline{y}_n \mid y \in \mathbb{Z}\}$, wird mit $\mathbb{Z}_n$ bezeichnet.

Modulo-Rechnung

Definition

$x \equiv y \pmod{n}$ genau dann, wenn $x - y$ ganzzahliges Vielfaches von n ist.

Definition (Restklassen)

Sei $y, n \in \mathbb{Z}$. Dann heisst die Menge $\{x \in \mathbb{Z} \mid x \equiv y \pmod{n}\}$ die Restklasse von y modulo n und wird als $\overline{y}_n$ geschrieben. Die Menge aller Restklassen modulo n, $\{\overline{y}_n \mid y \in \mathbb{Z}\}$, wird mit $\mathbb{Z}_n$ bezeichnet.

Definition

Seien $x, y, n \in \mathbb{Z}$. Dann definieren wir:

1. $\overline{x}_n + \overline{y}_n$ als $\overline{x + y}_n$;
2. $-\overline{x}_n$ als $\overline{-x}_n$; sowie
3. $\overline{x}_n \cdot \overline{y}_n$ als $\overline{x \cdot y}_n$.

Der Ring $\mathbb{Z}_6$

$+$	$\overline{0}_6$	$\overline{1}_6$	$\overline{2}_6$	$\overline{3}_6$	$\overline{4}_6$	$\overline{5}_6$
$\overline{0}_6$	$\overline{0}_6$	$\overline{1}_6$	$\overline{2}_6$	$\overline{3}_6$	$\overline{4}_6$	$\overline{5}_6$
$\overline{1}_6$	$\overline{1}_6$	$\overline{2}_6$	$\overline{3}_6$	$\overline{4}_6$	$\overline{5}_6$	$\overline{0}_6$
$\overline{2}_6$	$\overline{2}_6$	$\overline{3}_6$	$\overline{4}_6$	$\overline{5}_6$	$\overline{0}_6$	$\overline{1}_6$
$\overline{3}_6$	$\overline{3}_6$	$\overline{4}_6$	$\overline{5}_6$	$\overline{0}_6$	$\overline{1}_6$	$\overline{2}_6$
$\overline{4}_6$	$\overline{4}_6$	$\overline{5}_6$	$\overline{0}_6$	$\overline{1}_6$	$\overline{2}_6$	$\overline{3}_6$
$\overline{5}_6$	$\overline{5}_6$	$\overline{0}_6$	$\overline{1}_6$	$\overline{2}_6$	$\overline{3}_6$	$\overline{4}_6$

$\cdot$	$\overline{0}_6$	$\overline{1}_6$	$\overline{2}_6$	$\overline{3}_6$	$\overline{4}_6$	$\overline{5}_6$
$\overline{0}_6$	$\overline{0}_6$	$\overline{0}_6$	$\overline{0}_6$	$\overline{0}_6$	$\overline{0}_6$	$\overline{0}_6$
$\overline{1}_6$	$\overline{0}_6$	$\overline{1}_6$	$\overline{2}_6$	$\overline{3}_6$	$\overline{4}_6$	$\overline{5}_6$
$\overline{2}_6$	$\overline{0}_6$	$\overline{2}_6$	$\overline{4}_6$	$\overline{0}_6$	$\overline{4}_6$	$\overline{2}_6$
$\overline{3}_6$	$\overline{0}_6$	$\overline{3}_6$	$\overline{0}_6$	$\overline{3}_6$	$\overline{0}_6$	$\overline{3}_6$
$\overline{4}_6$	$\overline{0}_6$	$\overline{4}_6$	$\overline{2}_6$	$\overline{0}_6$	$\overline{4}_6$	$\overline{2}_6$
$\overline{5}_6$	$\overline{0}_6$	$\overline{5}_6$	$\overline{4}_6$	$\overline{3}_6$	$\overline{2}_6$	$\overline{1}_6$

Der Ring $\mathbb{Z}_6$

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	4	2
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Diskretes-Logarithmus-Problem

- Sei $g \in \mathbb{R}$ und $n \in \mathbb{N}$.
  - Das Berechnen von $h := g^n \in \mathbb{R}$ ist schwer: Ergebnis ist riesig
  - Den Exponent n aus h und g bestimmen ist einfach:

$$n = \log_g h = \frac{\log_{10} h}{\log_{10} g}$$

Diskretes-Logarithmus-Problem

- Sei $g \in \mathbb{R}$ und $n \in \mathbb{N}$.
  - Das Berechnen von $h := g^n \in \mathbb{R}$ ist schwer: Ergebnis ist riesig
  - Den Exponent n aus h und g bestimmen ist einfach:

$$n = \log_g h = \frac{\log_{10} h}{\log_{10} g}$$

Dezimalstellen zählen liefert erste Idee für n!

Diskretes-Logarithmus-Problem

- Sei $g \in \mathbb{R}$ und $n \in \mathbb{N}$.
  - Das Berechnen von $h := g^n \in \mathbb{R}$ ist schwer: Ergebnis ist riesig
  - Den Exponent n aus h und g bestimmen ist einfach:

$$n = \log_g h = \frac{\log_{10} h}{\log_{10} g}$$

    Dezimalstellen zählen liefert erste Idee für n!
- Sei p prim, $g \in \{2, \ldots, p-1\}$ und $n \in \mathbb{N}$
  - Das Berechnen von $h := g^n \bmod p$ ist einfach
  - Den Exponent n aus h und g bestimmen ist schwer

Diskretes-Logarithmus-Problem

- Sei $g \in \mathbb{R}$ und $n \in \mathbb{N}$.
  - Das Berechnen von $h := g^n \in \mathbb{R}$ ist schwer: Ergebnis ist riesig
  - Den Exponent n aus h und g bestimmen ist einfach:

$$n = \log_g h = \frac{\log_{10} h}{\log_{10} g}$$

    Dezimalstellen zählen liefert erste Idee für n!
- Sei p prim, $g \in \{2, \ldots, p-1\}$ und $n \in \mathbb{N}$
  - Das Berechnen von $h := g^n \bmod p$ ist einfach
  - Den Exponent n aus h und g bestimmen ist schwer
- Das Problem «finde n aus h und g modulo p» heisst Diskretes-Logarithmus-Problem

Binäre Exponentiation

Berechne

$$3814^{4361} \bmod 10^4$$

Binäre Exponentiation

Berechne

$$3814^{4361} \bmod 10^4$$

- Naiv multiplizieren und modulo 10^4 reduzieren: 4360 Multiplikationen modulo 10^4
- In der Kryptographie haben Exponent und Modulus hunderte Dezimalstellen
- Naiv multiplizieren ist viel zu langsam!

Binäre Exponentiation

Berechne

$$3814^{4361} \bmod 10^4$$

- Naiv multiplizieren und modulo 10^4 reduzieren: 4360 Multiplikationen modulo 10^4
- In der Kryptographie haben Exponent und Modulus hunderte Dezimalstellen
- Naiv multiplizieren ist viel zu langsam!

$\longrightarrow$ binäre Exponentiation kann dies viel schneller!

Binäre Exponentiation 1/4: Berechne $3814^{4361} \bmod 10^4$

$$
\begin{aligned}
& 4361 \\
&= 2180 \cdot 2 + 1 \\
&= (1090 \cdot 2) \cdot 2 + 1 \\
&= ((545 \cdot 2) \cdot 2) \cdot 2 + 1 \\
&= (((272 \cdot 2 + 1) \cdot 2) \cdot 2) \cdot 2 + 1 \\
&= ((((136 \cdot 2) \cdot 2 + 1) \cdot 2) \cdot 2) \cdot 2 + 1 \\
&= (((((68 \cdot 2) \cdot 2) \cdot 2 + 1) \cdot 2) \cdot 2) \cdot 2 + 1 \\
&= ((((((34 \cdot 2) \cdot 2) \cdot 2) \cdot 2 + 1) \cdot 2) \cdot 2) \cdot 2 + 1 \\
&= (((((((17 \cdot 2) \cdot 2) \cdot 2) \cdot 2) \cdot 2 + 1) \cdot 2) \cdot 2) \cdot 2 + 1 \\
&= ((((((((8 \cdot 2 + 1) \cdot 2) \cdot 2) \cdot 2) \cdot 2) \cdot 2 + 1) \cdot 2) \cdot 2) \cdot 2 + 1 \\
&= (((((((((4 \cdot 2) \cdot 2 + 1) \cdot 2) \cdot 2) \cdot 2) \cdot 2) \cdot 2 + 1) \cdot 2) \cdot 2) \cdot 2 + 1 \\
&= ((((((((((2 \cdot 2) \cdot 2) \cdot 2 + 1) \cdot 2) \cdot 2) \cdot 2) \cdot 2) \cdot 2 + 1) \cdot 2) \cdot 2) \cdot 2 + 1 \\
&= (((((((((((1 \cdot 2) \cdot 2) \cdot 2) \cdot 2 + 1) \cdot 2) \cdot 2) \cdot 2) \cdot 2) \cdot 2 + 1) \cdot 2) \cdot 2) \cdot 2 + 1
\end{aligned}
$$

Binäre Exponentiation 2/4: Berechne $3814^{4361} \bmod 10^4$

- Also: $4361 = 2^{12} + 2^8 + 2^3 + 2^0$
- 4361 hat Binärdarstellung 1000100001001_2

Binäre Exponentiation 2/4: Berechne $3814^{4361} \bmod 10^4$

- Also: $4361 = 2^{12} + 2^8 + 2^3 + 2^0$
- 4361 hat Binärdarstellung 1000100001001_2
- Binäre Exponentiation:

$$x^{4361} = ((((((((((((x^2)^2)^2)^2 \cdot x)^2)^2)^2)^2)^2 \cdot x)^2)^2)^2 \cdot x$$

Binäre Exponentiation 2/4: Berechne $3814^{4361} \bmod 10^4$

- Also: $4361 = 2^{12} + 2^8 + 2^3 + 2^0$
- 4361 hat Binärdarstellung 1000100001001_2
- Binäre Exponentiation:

$$x^{4361} = ((((((((((((x^2)^2)^2)^2 \cdot x)^2)^2)^2)^2)^2 \cdot x)^2)^2)^2 \cdot x$$

- Konkret: 3814^{4361} ist gleich

$$((((((((((((3814^2)^2)^2)^2 \cdot 3814)^2)^2)^2)^2)^2 \cdot 3814)^2)^2)^2 \cdot 3814$$

Binäre Exponentiation 3/4: Berechne $3814^{4361} \bmod 10^4$

$$
\begin{aligned}
3814^2 &= 14546596 \equiv 6596 \bmod 10^4;\\
6596^2 &= 43507216 \equiv 7216 \equiv 3814^4 \bmod 10^4;\\
6596^2 &= 52070656 \equiv 656 \equiv 3814^8 \bmod 10^4;\\
656^2 &= 430336 \equiv 336 \equiv 3814^{16} \bmod 10^4;\\
336 \cdot 3814 &= 1281504 \equiv 1504 \equiv 3814^{17} \bmod 10^4;\\
1504^2 &= 2262016 \equiv 2016 \equiv 3814^{34} \bmod 10^4;\\
2016^2 &= 4064256 \equiv 4256 \equiv 3814^{68} \bmod 10^4;\\
4256^2 &= 18113536 \equiv 3536 \equiv 3814^{136} \bmod 10^4;\\
3536^2 &= 12503296 \equiv 3296 \equiv 3814^{272} \bmod 10^4;\\
3296^2 &= 10863616 \equiv 3616 \equiv 3814^{544} \bmod 10^4;\\
3616 \cdot 3814 &= 13791424 \equiv 1424 \equiv 3814^{545} \bmod 10^4;\\
&\vdots
\end{aligned}
$$

Binäre Exponentiation 4/4: Berechne $3814^{4361} \bmod 10^4$

$$\vdots$$

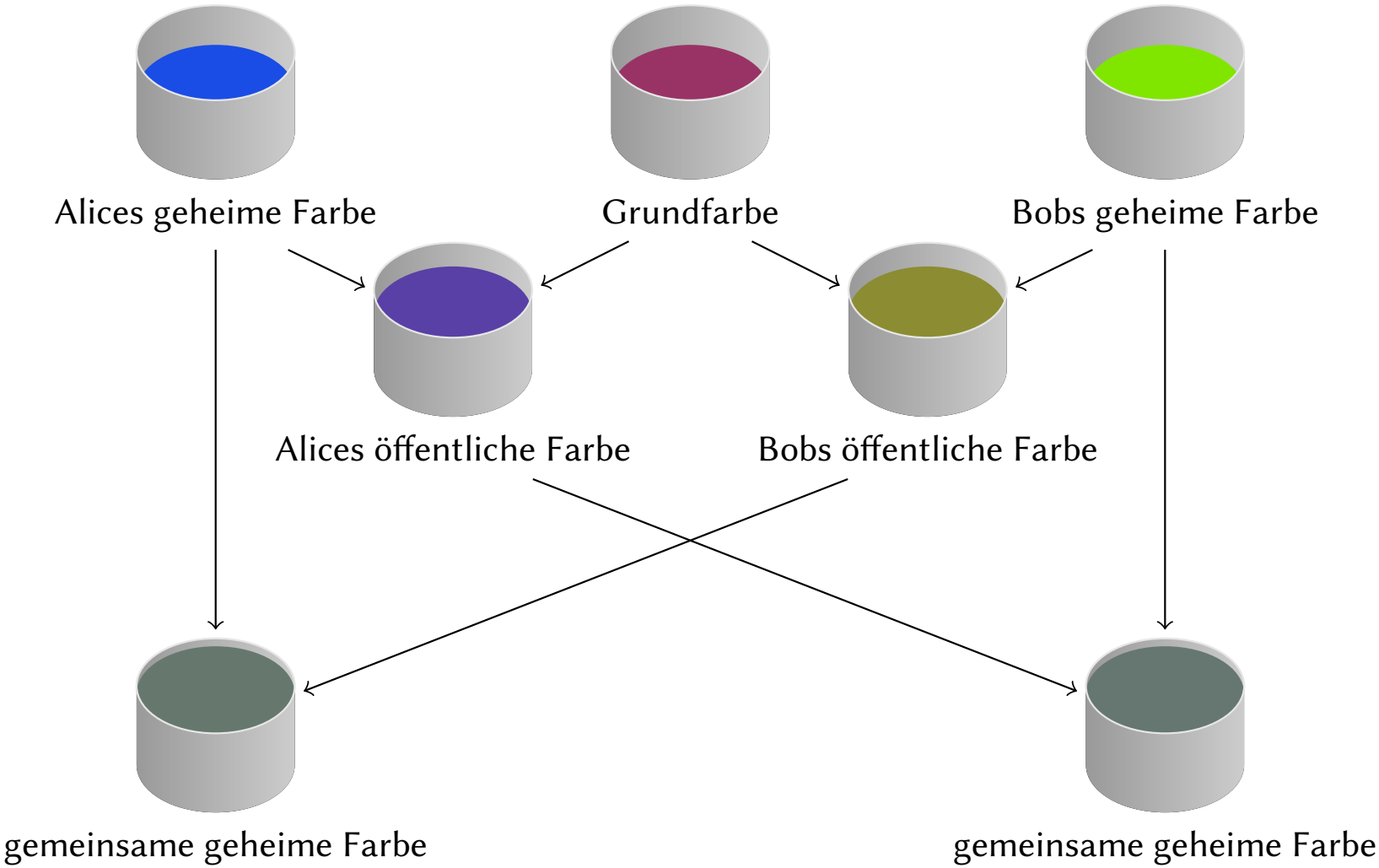
$$3616 \cdot 3814 = 13791424 \equiv 1424 \equiv 3814^{545} \bmod 10^4;$$
$$1424^2 = 2027776 \equiv 7776 \equiv 3814^{1090} \bmod 10^4;$$
$$7776^2 = 60466176 \equiv 6176 \equiv 3814^{2180} \bmod 10^4;$$
$$6176^2 = 38142976 \equiv 2976 \equiv 3814^{4360} \bmod 10^4;$$
$$2976 \cdot 3814 = 11350464 \equiv 464 \equiv 3814^{4361} \bmod 10^4.$$

$$\Longrightarrow 3814^{4361} \equiv 464 \pmod{10^4}$$

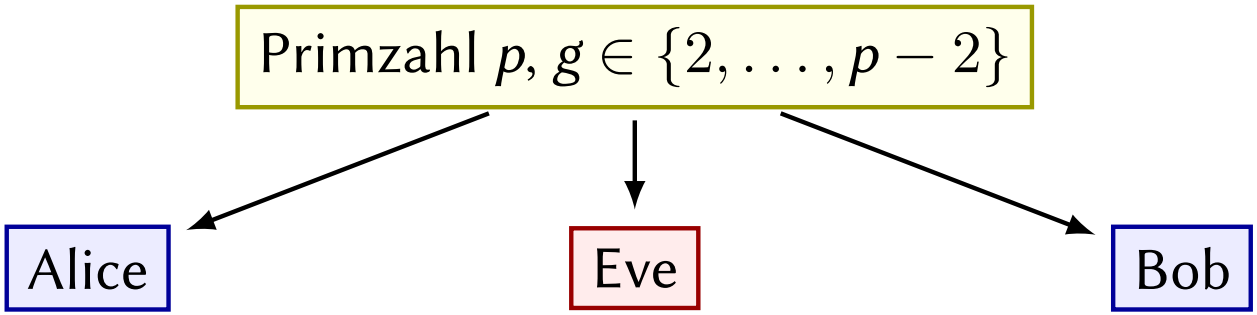
3814^{4361} ohne Modulo: 15'619 Dezimalstellen

25187407250493852220376303320625205510352210929241953573176904207077458609896897775354501872506869631426694310886061460667795845887826611631509646295815325974746169433640998165713499652818291391169292225768059397060832362423560653066705588687665794992189116053974756596536393081295331118860883516809150141693643310416135154667631498361017202908719187754270878530042810662684178318401427248442314066458022311914458039513955719740137139205192656580627423859182097813692375390169250961020712894923701430958659671917235736935040941452786857094299636397397263077416768690374409262196203012547017273355601594248284800484406802619869733960131980583498607224489262046893625541418708473665395060134614293143636125237427146653261943843835759277819602067654369788865780594774805993375453089080395460960312954149875024800420778299763524516455756051571705112345253437423297614242030552389109940687068703438329670338421556170400413497526285623538987617200166967576463645647737720009475413571561444653241826153783771077664838488019703258309195317842643282322471861898585597390330138739848800365307238935407460089939162434166887960337125949649077131367950906594698826451661934382465149491789235805234278556232703828524180911090542370364340263852496608949329671726672911666653291784516141778866727013388617198259674297061024997456450398172777433732594581659630020130659451062155428919519744807819823615396150528586237207912089017751147427443907405647804054120769583839260504606044075729742661602563484517946795896685182565147222679948907995894449623187801861150739711534633411266156983912437532963387266645200015568890423868545318413732560733596558544934535051001360048446970461204027780539589108701660433186616771142111227480440292305994067672615224372134311396973754810710409663389494727592122760825323866773114572441282195761528329938427854333309791365667225984248117959770083687325999542243725228401885431641853690085533185395399975222265365925932947818794255244725992775467365053668251500892865504777884762217534345810302090766441297057898855549471461328378546437745567008023918202964829613540390096349188596468691688863431264883185233027523789429946237280677844928363319491993842462453922882875727877313774756338018826332041205722826909453626255307510531605937325212415536740456725026634874843111340052678685256562504414585243909383858746086951003076760686578113482469250920790693498337476649545087698126823986470382026445479223053957856404454984176635902000440364138345310031651524377427470253737116411354173736607112601456951746429645384322821797133768332226417066283730157294200892124165127906667783374382090823894086964691466403664150405974038077151793979422937242236374847286900123115109003768314592854577162267039239355450794883123777452872466779800896272257793068759879358613097497341265911809440962723701735896311689212045848864408275508822787437091796902592692368018469387598351586813840170134089641276319105380994079159985395594592030829385413445513003107431571716215230780498331507000214282641923761245432639289646066698426871869220155311558714716799098397517292568156894780229596586299435790397238360518573539002343744157640851355486930823692093335215286735611848882481478961407192851304787740613742008090125836841741315391216267145546669131263121683137585811255623671010700251665375195457809296199215037902292261829069571730495273405971743995532765338365931953069956295762433395167145153961602115161775195228745524178570343655428555893602445645956172946118256681825531752458020206366610568285784998306746947725923873642690224718897653862213768283251728759084813446402155229221476813410937926575662349571499240499900679337681228080333761246463237425585535402273024767025426586710236153246418256188830063819092318006427802880155679122295441152262707293719458883677872008302208006082176508660926732771172050760680632519747944879500237066631353373633237205657969542131637962264393899992833170832258511804789484317713679655941431544977006749132557808962560553909598835094834977695952388398093526290005706264997098503753029543766281334084100912172995978623239041138186737710592706926672148068092998738219877715922943700200264067699732705791776325987853930908814583247179911362718921826950868729663036087081732948862270540055375844105167324087462384745994486203856096541156653926857829323174075883215337069581478858018685905123927895644805707745339969613267222295905136308700890517960957613245829558786371612535054349797853318474656281111901604497012304943333956475739244168839534918071607973133874295019644825461933220336882761413949344245153247421441077551065748337010441886505957173790673763070028335695425172547966076362214185311183776970700459605604105344739961680732402022509566284354899481012719839787354385050547072908262901983925069620932895413709802607420810653910710809836372841021406137590718455812075801576893867649226351937730298992582808692778515929046861288211255773745601661251380255239371729476954091088167285253944644235716756610412508426041855558347183129539072853604571686063198848356585182922988884384718195040895062498943954604499960260193656063937381729073640504555053151856268457787321651914027311895184787710257946066745655016208096835991066628468374599124283402698290045740976827505722703857861506361237199688754424449575004044423779781312639431953731046692860655483059196234579703982324461067923152457643101323738362800506501872560982423496594600643033044805498088410751237195821268803924970256832963434991315048628602866118774358941092658309813857490585899420076855071406695215365274164852938044402643183433980072157660760060919600408344371627305506608350507555329799582699935374956374386655584427047128126487847544274518054480942797430209981141274961657126480586122632251358788445583132754361400705756212710448835833073461713252206470741769012729800722359429042187570160505055108558177034055191156178795574403183555174603370664452050421580260157776769610034535716597945055551788010145862041724807947630445672792857379387421498925676515676317262704205586178250937979707681011572631114427480060222730603847959616575134841410635110257451586243077019654896663095341445068880556753966071350453983141887752547014979928145816458907471206109246411208882105545565710152330489617633846884269001761058792090121083420400852205695355581870340790435190794477254461107237479752067834349788088846768067421789334768386997165191969771332324159384742081867176567397029988546910963341923663134722111741655746569450438629437690200580141192275630116656006982687336509602386277815938508492733921070119930824415025072980403492609827954448912510612934349016042738140886786623871420774894504995808915374955658620059584117095330570499032640463314027565837028312559491400649581644798095518065980163192165276571525971196197671415320138282920290522623030481647643051084894546793006944139741514337159482558930451124951230325644848303582407091849590434431803894513691743263822159083877035551917201758847088203721614359301470838212251435641773420013227848880474213131973415521863648711082368521609417191054688347765461645213340201613323090658925367922724683280201892842061755600739524361236981150557703286999061740538830677608182282288169463709390024452027465762158310081239825592319442010222666440790657201896938569117396195094878848906619990273129451962639409123507110392907837748426510303134656233196708895782324923366396863837978805876343394130767328793883683608450095705250850827202387781441951304552760683916204607369538554845094500820361642136553175282094611073976122679335874522340100553389248379824989969080473900924202117472715137682121433685263358499517886066750555122664036779264787349785093951023665509030666159537969624120534463664637453003000170180622949282440932809343581891089349296333769341665716097244978102437402568508341408463521984302567364432474827447235783565438635048307332352879055324971324902611632640157185977426850209117100229759621307239518511573860622881830750220571648491239955231773483341031733242127808911392175898633047984309312919003276281267188838725209582108854402555736868024333769976752789423556230739121462587972337865527542791185100050826584711527714979143735565527940166948367588739139208885266437501346350736505610103497667153178186853094236456866024219873211360430621563886623826059072341297572317814689941460488058063819193248192240908864693221962534553581637969795554244239715359850804675547557173693207138479852253714993402892118171348740129508521102056025430606872295951332337770405313078010346130825830415161821272769881719032484072561835002992472228836861446533521432026992811900873747127471937752651640194990697735825805774030450342688714408869660536562779185940533237792665805440755589000108661490120721561190169042268667385150404515827258030684800368967260237768624140227551634973497894720657756401949906977358258057740304503426887144088696605365627791859405332377926658054407555890001086614901207215611901690422686673851504045158272580306848003689762202377686241446553352143202699281190087374712747193775265164019499069773582580577403045034268871440886966053656277918594053323779266580544075558900010866149012072156119016904226866738515040451582725803068480036896726023776862414202755163497343497994280657756338720212268356239887503955307834383460526968386947881431560555163832013513737392696401437840097743670367360521672457870054241677229018793609783625418179270104524576509332686142210784183820695367884285044890591182027172996871129035301643899956019380810855482501704686050213566000872589313847330888392688274112918252426091515355325410590220051686481607662117463253404089614787882958075821246417728169729101639440007300935062263966624526586972854649549776779934931318347005843025323739952714772045333549191399851809741452557728340603649076673999931752707392991973612456492717267488393095077641298427389406809107883542391236761286976292025490568024078735839860640278569610380723928574713678577044713892808910224904085054522196041324305241660665068695736111644025539425676745334222061523541218841978899540785547990486870284179768020871232133530014690011982772305147293047785705258915205170147604367132133551486358233158516497415709410575319173045187773824043396334189686854111776017006093976664065159502332866376845794198770673507339839764495968249357342488070361499833752208466757161786751831465665527192756740225455133962808406731889467128837757936155114348824953421513562571680276039791187092173978754090837641112601864048674364810033511450092238107722230467849306147474691889436827280693094479995761358569595581121688459241286996669894293893559982894654277817222356385817106342510955907513614422195182781777691340695268703388102275974629526629109146126512786114597882651822661958440253742045300061117094929594333971465779664336453914317893862691600532495005267253772699007912794046783882231770688567740564914916339718455878870267021560108666755785172182828047963413149021093438681199641621122839186379228542869273955105408518353435998115485245712844917869196198141046024851607770367254101086420508372707228686632782433020008535292682787143443963820258122781551300431034441481645653643672105629268592728872503937078968146377351321930557553170311762865533427683570604189372117222665230772848554179227581346646493240070067115878534748320283334258865056164585298431310761234819721013043104463361723996814833870400068497331156167626498611933322734242838230078553524018746479862977181969370297192503181305196339697208300918244530959422623889886161263269385265174981474375161606743002839759716085055160846850391508552507129989142778351157193998152228885727873864596115547626680834059323763041400510440099827343430002848461259757902186910447891016923459910972004571161450538966965457225512879837434209079209094102285627145306409229179677915398367763583189499676353511346464122870459095576443344044678478104841236341711213937389761915237540742051162981225576642769153167843469235917460806978133956919609321779895404185641776670381409581854901888776785115322768629258967145902685415850468867145252875806015835352897324586223079104047205796394894144606511101082160730247965808324136023977847344597202372209943155465310095453219145532605524926228313981878704972259369556853772958263312846842197326590004832288539344503085529365051218991379159079980256203678018566579795336976972142269988444738765609004864601373041216322676652467874390431980533214344289612452287668042688412924666834852562965801162425316074899388624982058168802247902288747608177948387945675956355662568196900475946252832690177040487841647766951518260634198165297390198813646994481710778542182019408771993891458444022761746093369612612457394982842866586404699855741305661805749787716764290530790241523307459317985397045703398087087910244954597515209406708583129992576639626580567967166047101970687947602054943592998502441332913109966847364634568398917295527771818183836324065877950464

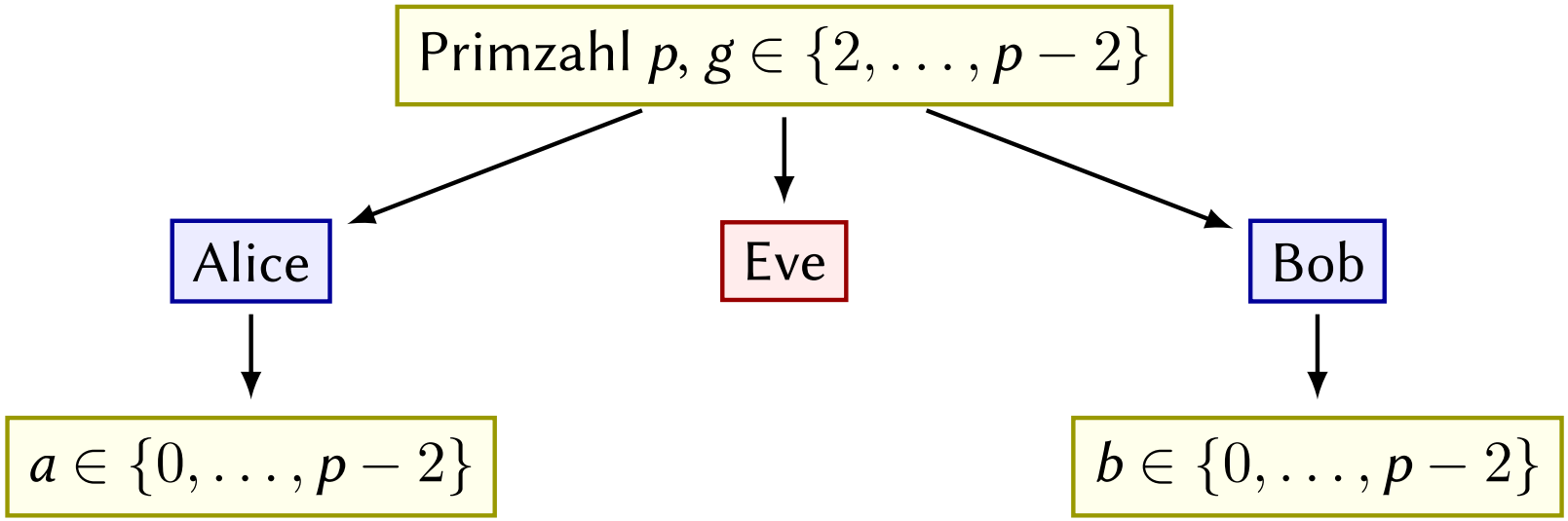
Diffie-Hellman-Schlüsselaustausch mit Farben



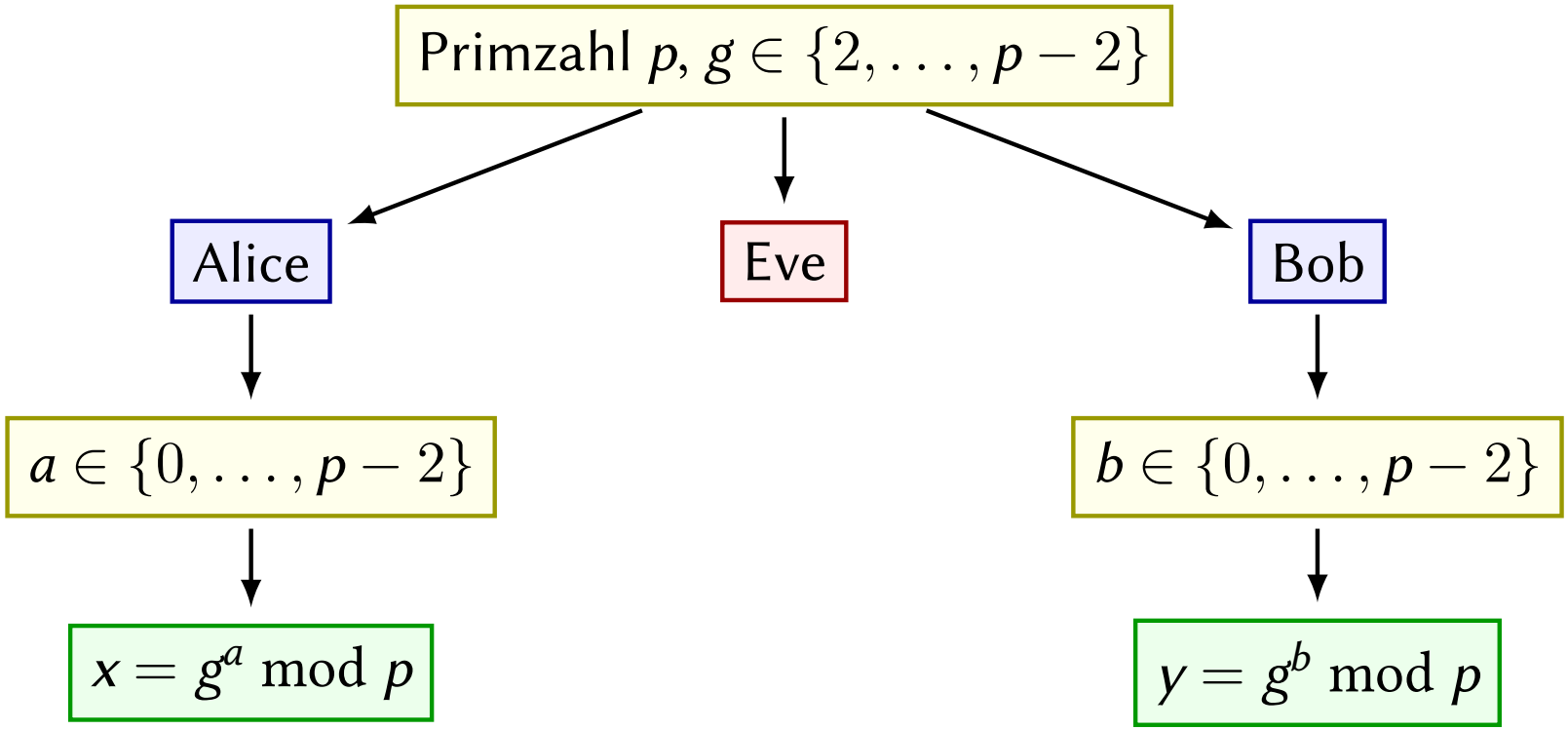
Diffie-Hellman-Schlüsselaustausch mit Modulo-Rechnung



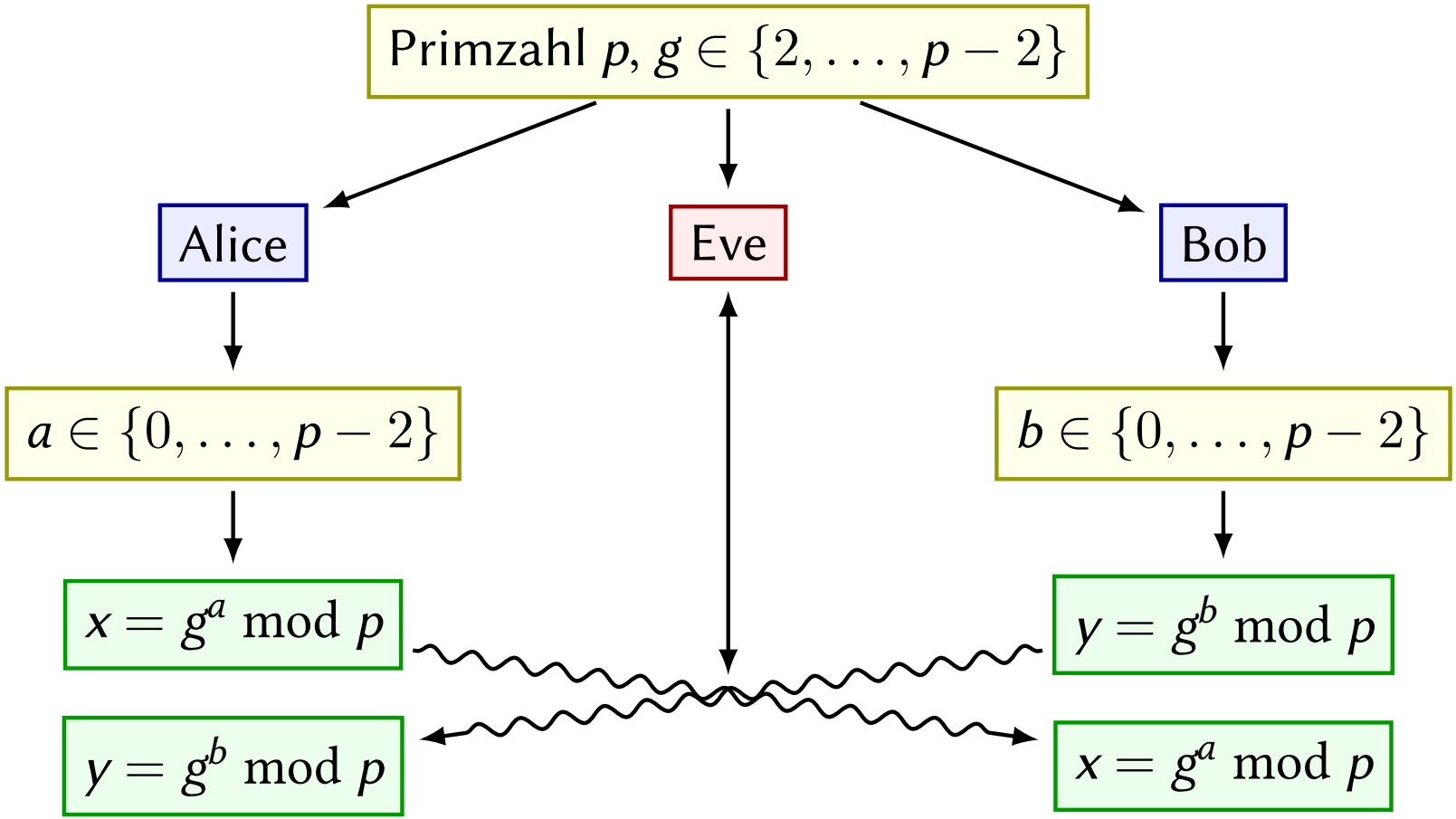
Diffie-Hellman-Schlüsselaustausch mit Modulo-Rechnung



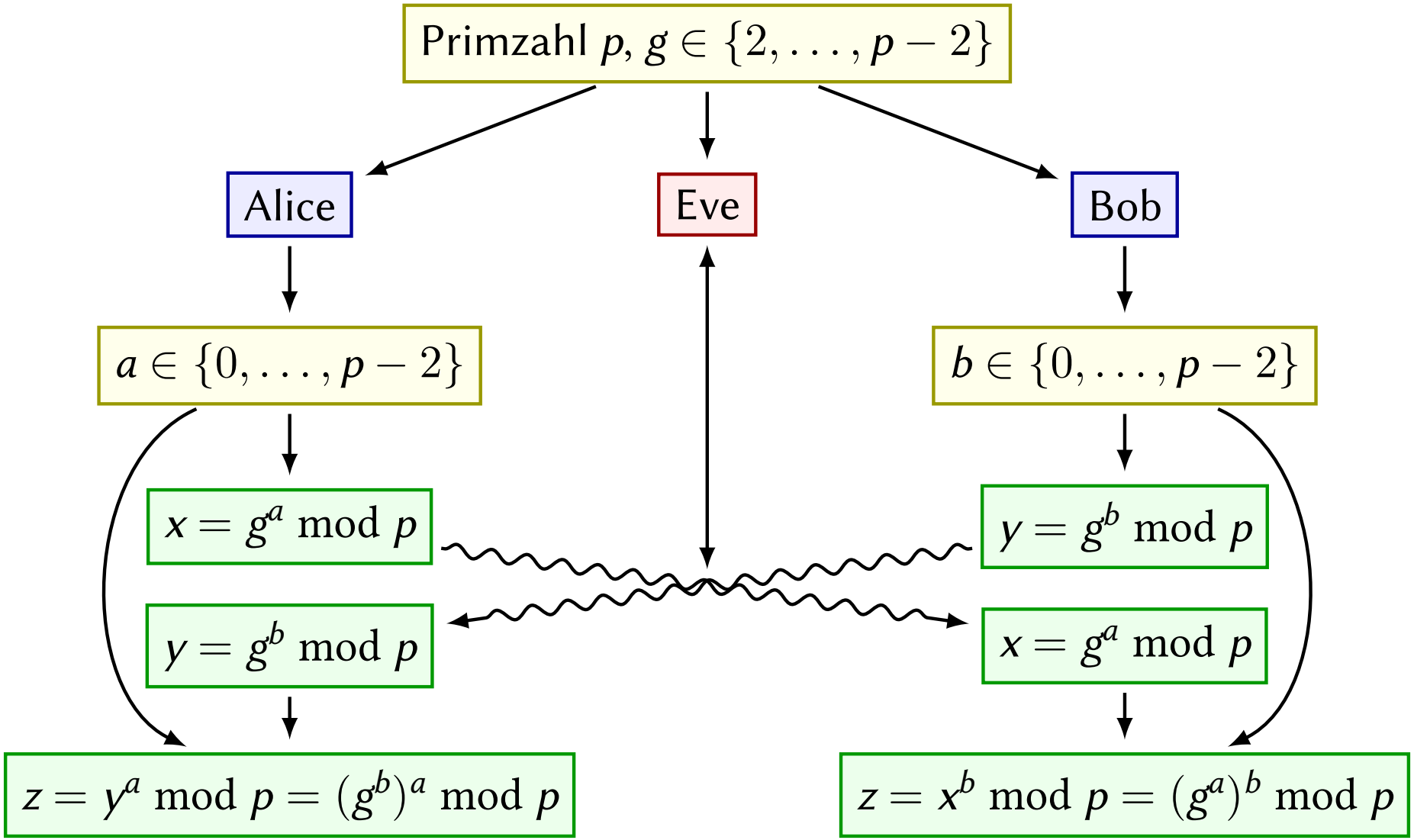
Diffie-Hellman-Schlüsselaustausch mit Modulo-Rechnung



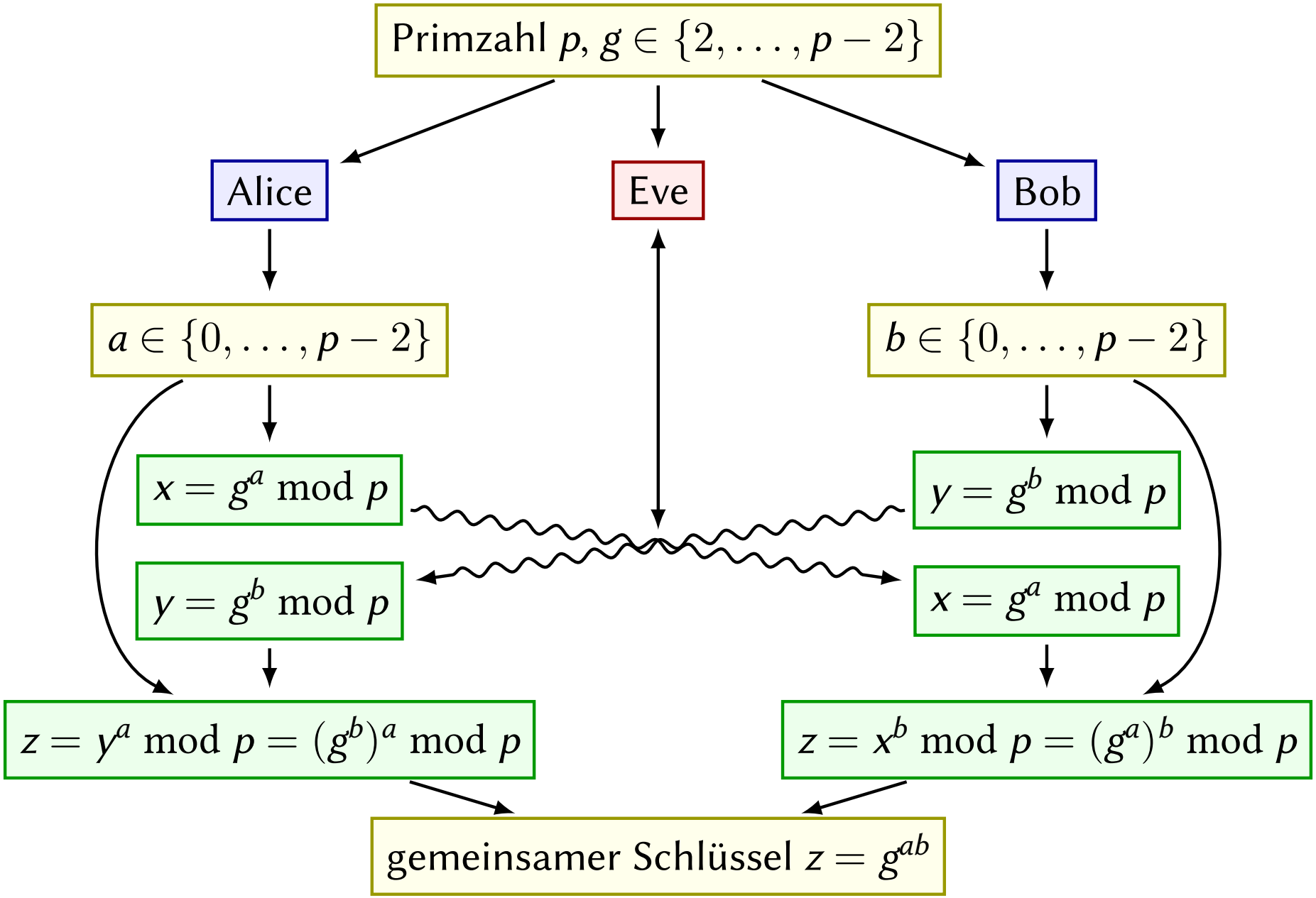
Diffie-Hellman-Schlüsselaustausch mit Modulo-Rechnung



Diffie-Hellman-Schlüsselaustausch mit Modulo-Rechnung



Diffie-Hellman-Schlüsselaustausch mit Modulo-Rechnung



Ausblick

Mathematische Probleme für asymmetrische Kryptographie:

- Faktorisieren von Zahlen
- Diskretes-Logarithmus-Problem modulo p
- Diskretes-Logarithmus-Problem bei elliptischen Kurven

Ausblick

Mathematische Probleme für asymmetrische Kryptographie:

- Faktorisieren von Zahlen
- Diskretes-Logarithmus-Problem modulo p
- Diskretes-Logarithmus-Problem bei elliptischen Kurven

Quantencomputer können diese Probleme sehr effizient lösen!

Ausblick

Mathematische Probleme für asymmetrische Kryptographie:

- Faktorisieren von Zahlen
- Diskretes-Logarithmus-Problem modulo p
- Diskretes-Logarithmus-Problem bei elliptischen Kurven

Quantencomputer können diese Probleme sehr effizient lösen!

Post-Quanten-Kryptographie

- Probleme, die man auch mit Quantencomputer nicht gut lösen kann

Ausblick

Mathematische Probleme für asymmetrische Kryptographie:

- Faktorisieren von Zahlen
- Diskretes-Logarithmus-Problem modulo p
- Diskretes-Logarithmus-Problem bei elliptischen Kurven

Quantencomputer können diese Probleme sehr effizient lösen!

Post-Quanten-Kryptographie

- Probleme, die man auch mit Quantencomputer nicht gut lösen kann
  - kurze Vektoren in Gittern
  - Dekodieren von fehlerkorrigierenden Codes
  - Isogenien von supersingulären elliptischen Kurven

Ausblick

Mathematische Probleme für asymmetrische Kryptographie:

- Faktorisieren von Zahlen
- Diskretes-Logarithmus-Problem modulo p
- Diskretes-Logarithmus-Problem bei elliptischen Kurven

Quantencomputer können diese Probleme sehr effizient lösen!

Post-Quanten-Kryptographie

- Probleme, die man auch mit Quantencomputer nicht gut lösen kann
  - kurze Vektoren in Gittern
  - Dekodieren von fehlerkorrigierenden Codes
  - Isogenien von supersingulären elliptischen Kurven
- Bisherige Lösungen: langsam und speicherhungrig im Vergleich zu RSA & Co
- Aktives Forschungsgebiet!

Guten Start ins Studium!