

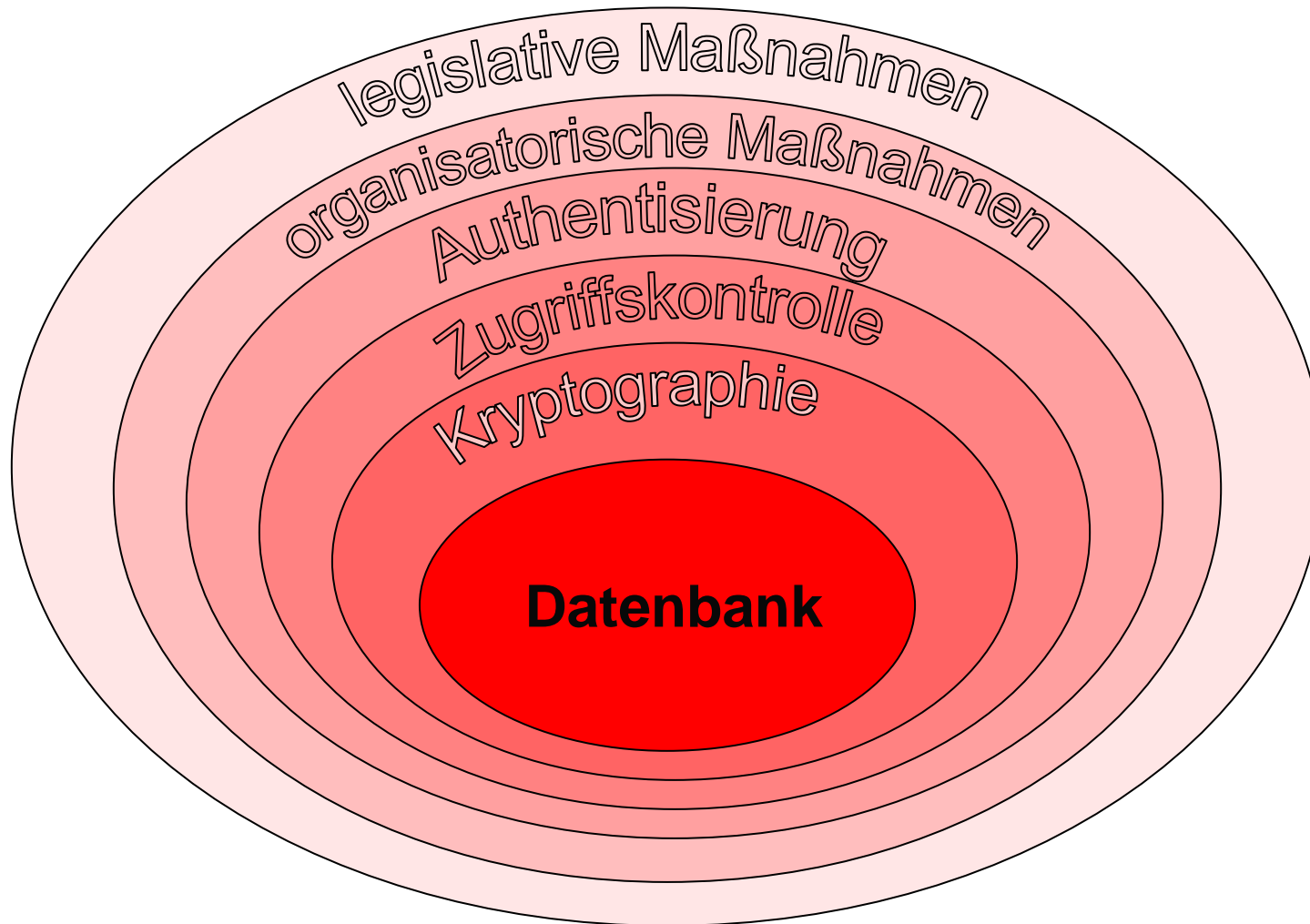
Datenbanksysteme 2011

Kapitel 17: Sicherheit

Oliver Vornberger

Institut für Informatik
Universität Osnabrück

Datenschutz



Legislative Maßnahmen

**Gesetz
zum Schutz
vor Missbrauch
personenbezogener
Daten
1977**

Organisatorische Maßnahmen

- bauliche Maßnahmen
- Pförtner
- Ausweiskontrolle
- Diebstahlsicherung
- Alarmanlage

Authentisierung

- Magnetkarte
- Stimmanalyse
- Fingerabdruck
- Passwort
- dynamisches Passwort

Zugriffskontrolle durch Berechtigungsmatrix

Benutzer	Ang-Nr	Gehalt	Leistung
A (Manager)	R	R	RW
B (Personalchef)	RW	RW	R
C (Lohnbüro)	R	R	-

Zugriff (A, Gehalt):
R: Gehalt < 10.000
W: Gehalt < 5.000

Zugriffskontrolle durch Sichten

```
define view v(angnr, gehalt) as  
select angnr, gehalt from angest  
where gehalt < 3000
```

Zugriffskontrolle durch Abfrageeinschränkung

```
deny (name, gehalt) where gehalt > 3000
+
select gehalt from angest where name = 'Schmidt'
=
select gehalt from angest
where name = 'Schmidt' and not gehalt > 3000
```


Zugriffsrechte in SQL-92

```
grant { select |
        insert |
        delete |
        update |
        references |
        all }
on <relation> to <user> [with grant option]
```

A: grant read, insert on angest to **B** with grant option

B: grant read on angest to **C** with grant option

B: grant insert on angest to **C**

Obacht bei Recht auf Fremdschlüssel:

Probeweises Einfügen kann Schlüssel finden !

```
create table Agententest(Kennung character(3) references Agenten)
```

Revoke-Anweisung

```
revoke { select |  
        insert |  
        delete |  
        update |  
        references |  
        all }  
on <relation> from <user>
```

B: revoke all on angest from **C**

Entzug eines Grant

... als wenn es nie gewährt worden wäre:

A: grant read, insert, update on angest to **D**

B: grant read, update on angest to **D** with grant option

D: grant read, update on angest to **E**

A: revoke insert, update on angest from **D**

D verliert nur sein insert-Recht, weil update von B erh.

E verliert keine Rechte (weil indirekt von B erhalten)

B: revoke update on angest from **D**

D verliert update-Recht

E verliert update-Recht

Auditing

```
audit delete any table
```

```
noaudit delete any table
```

```
audit update on professoren  
whenever not successful
```

Verschlüsselung

z3619#d7%isör
Seid Anjer

Caesar-Chiffre

Verschiebe Buchstaben im Alphabet

z.B. 4

C A E S A R

G E I W E V

XOR-Verknüpfung

Klartext: 010010101110110

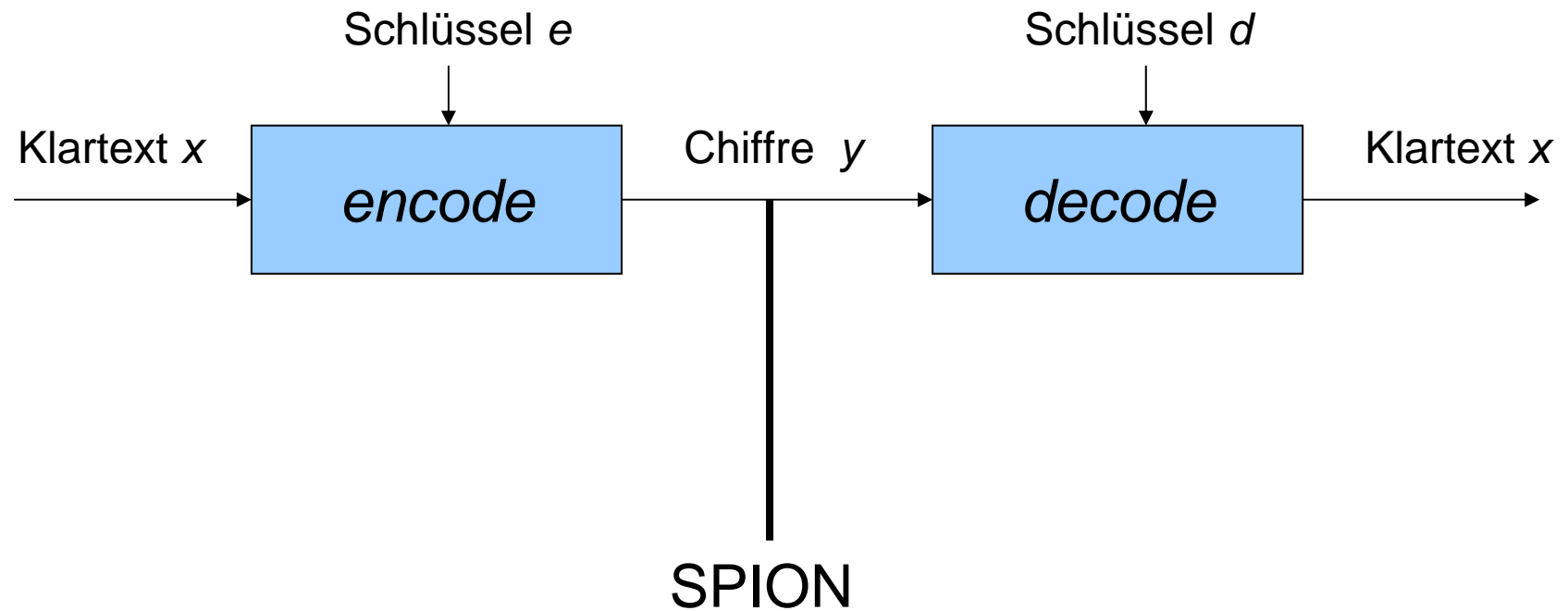
Schlüssel: 110110110110110

Chiffre: 100100011000000

Schlüssel: 110110110110110

Klartext: 010010101110110

Ablauf

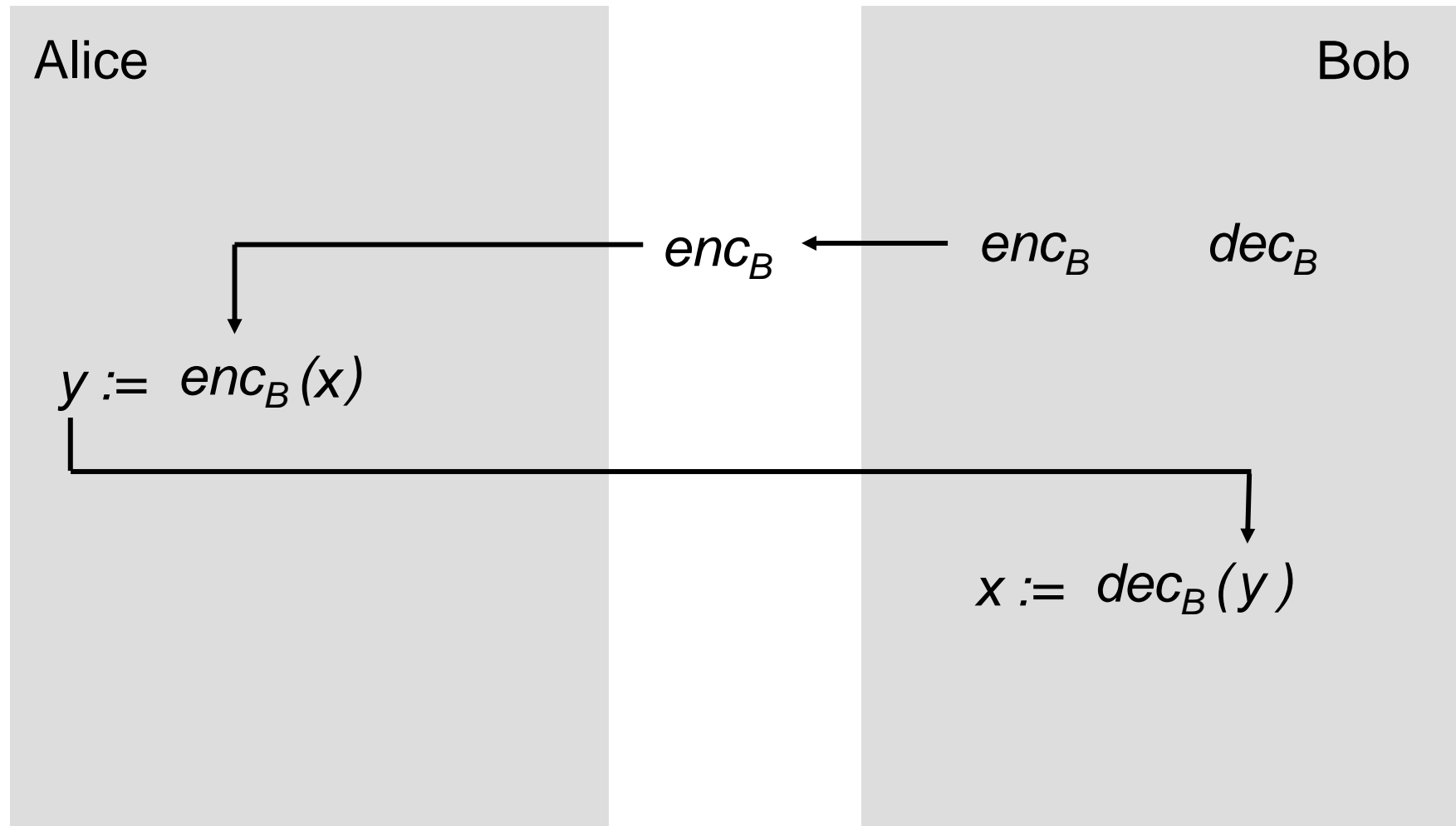


Diffie & Hellman, 1976

$$\textit{decode}(\textit{encode}(x)) = x$$

aus der Kenntnis von *encode*
läßt sich nicht *decode* ermitteln

Nachricht verschlüsseln



Einweg-Funktion

Cabarena	42347
Cadiz	996543
Caesar	784513
Carter	341123
Castrop	458944
C	5

Rivest, Shamir, Adleman, 1978:

Wähle 2 Primzahlen p, q

Bestimme $n := p \cdot q$

Wähle Zahl d relativ prim zu $\varphi(n) := (p-1) \cdot (q-1)$

Bestimme e mit $e \cdot d \equiv 1 \pmod{\varphi(n)}$

$$\text{encode}(x) := x^e \pmod{n}$$

$$\text{decode}(y) := y^d \pmod{n}$$

Beispiel mit 2-stelligen Primzahlen:

$$p := 11$$

$$q := 13$$

$$n := 143$$

$$d := 23$$

$$e := 47$$

$$\text{encode}(x) := x^{47} \bmod 143$$

$$\text{decode}(y) := y^{23} \bmod 143$$

Beispiel mit 200-stelligen Primzahlen:

p=899095310588366277174404228586414024566849766837212553005901900739450280241887356469178340
01445460697949352415335921952260900528540697407053331179637761895800615635806322855777396006
499513330486337609

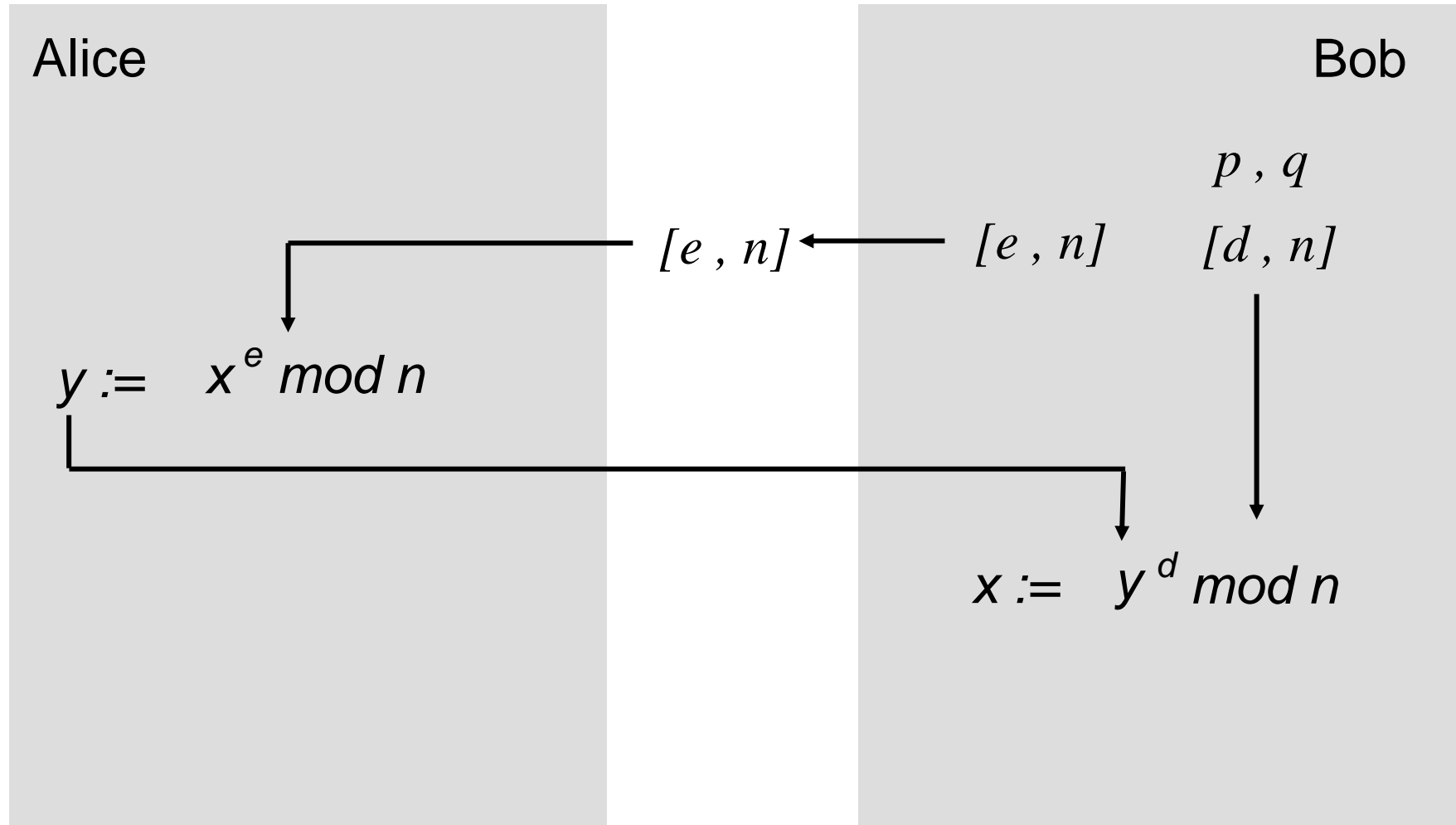
q=799021750781472446863793395126772763662312207522293560193498936718764209317443774306873658
12687754246830101282297574713772455933933867764022563251792393443769903948317050160321698561
025532877647684683

n=718396709185728164758130406575597352623217167087482423402776422026394961290886704476440994
80131986398124330716615728276265478293852457052897783239457461047674983301220394641493156652
06737745079315029030505846196489917568869335544777353689814016451189380595050450835091699231
54313966186550716311470774938467149320721564382277558501659803548182002418940885178176129421
9320404437751888461388903116142947

d=691288079298313420179509757559260912909411714295173215591611313470806161927060937609028421
00138662184459301019618950565163973523245851202287749007208501965412618330704286209316613491
55515945612960396000308199646278344377562606989931674080238238945773520492076314252906439396
12918561992617610661839159486351599606632765903498686713691135601407685940691700887034189568
0167331429079515342903719787052113

e=320609563217012599055965787364600473651115000782359791508086517839125482938194325978316198
29917499109195252931659284324831218397277144058830127546998961582106443297700554088899665948
07164754843416883200352765212163189383954679717196096719153707633822634088892728761608455440
7880875931958510259177246251661227907691999195827804405610391749679780186113

Nachricht verschlüsseln



Korrektheit

Satz von Fermat/Euler:

$$x \text{ relativ prim zu } n \Rightarrow x^{\varphi(n)} \equiv 1 \pmod{n}$$

Komplexität

$x^e \bmod n$

$$x^{13} = ((x^2 \cdot x)^2)^2 \cdot x$$

$$e \cdot d \equiv 1 \pmod{(p-1) \cdot (q-1)}$$

$$\text{ggt}(a,b) := \text{ggt}(b, a \bmod b)$$

$$(p-1) \cdot (q-1) \quad d$$

$$120 \quad 19$$

$$19 \quad 6$$

$$6 \quad 1$$

$$1 \quad 0$$

Primzahl erkennen

Prim [?] ∈ P

Prim ∈ NP

$\overline{\text{Prim}}$ ∈ NP

$\overline{\text{Prim}}$ ∈ RP

Primzahlen erzeugen

würfel ungerades x (500 Bit)

teste $x, x+2, x+4, \dots$

mittlerer Abstand $\ln(x) \Rightarrow \ln(2^{500}) \approx 350$

x ist Zeuge für die Zusammengesetztheit von n

n zusammengesetzt \Rightarrow mehr als $\frac{3}{4} n$ Zeugen

$z=0;$

repeat

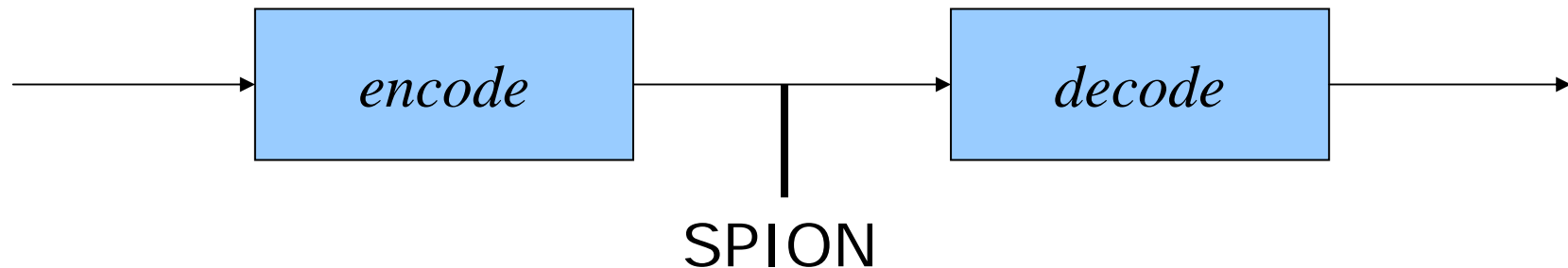
$z++;$

würfel x

until (x ist Zeuge für n) or ($z=50$)

Fehler = $\frac{1}{4}^{50} \approx 10^{-30}$

Sicherheit



Der Spion kennt e, n, y

Faktorisieren von n würde p und q liefern.

Damit könnte er d ausrechnen.

Aber: Faktorisieren von n dauert $n^{\sqrt{\frac{\ln \ln (n)}{\ln (n)}}}$ Schritte !

$$n = 2^{1000}$$

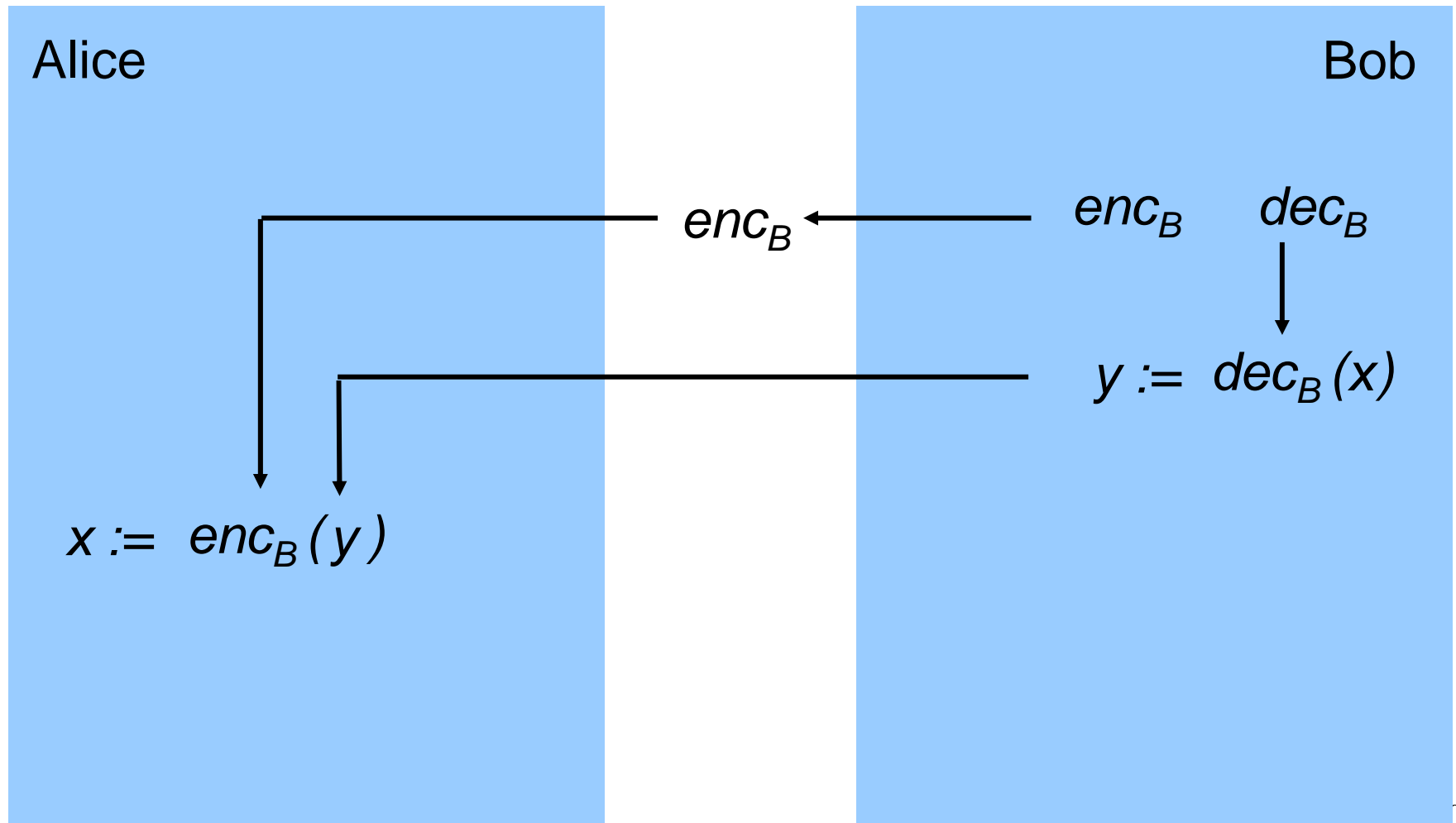
$$\Rightarrow n^{0.1} \text{ Schritte}$$

$$= 10^{30} \text{ Schritte} = 10^{13} \text{ Jahre (bei } 10^9 \text{ Schritte/sec)}$$

Reihenfolge vertauschen

$$\begin{aligned} \text{decode}(\text{encode}(x)) &= x \\ &= x^{ed} \bmod n \\ &= x^{de} \bmod n \\ &= \text{encode}(\text{decode}(x)) \end{aligned}$$

Nachricht signieren



Und wenn sie nicht gestorben sind,
entschlüsseln sie noch heute !