Primzahlen und Verschlüsselung

Thorsten Kleinjung

École Polytechnique Fédérale de Lausanne

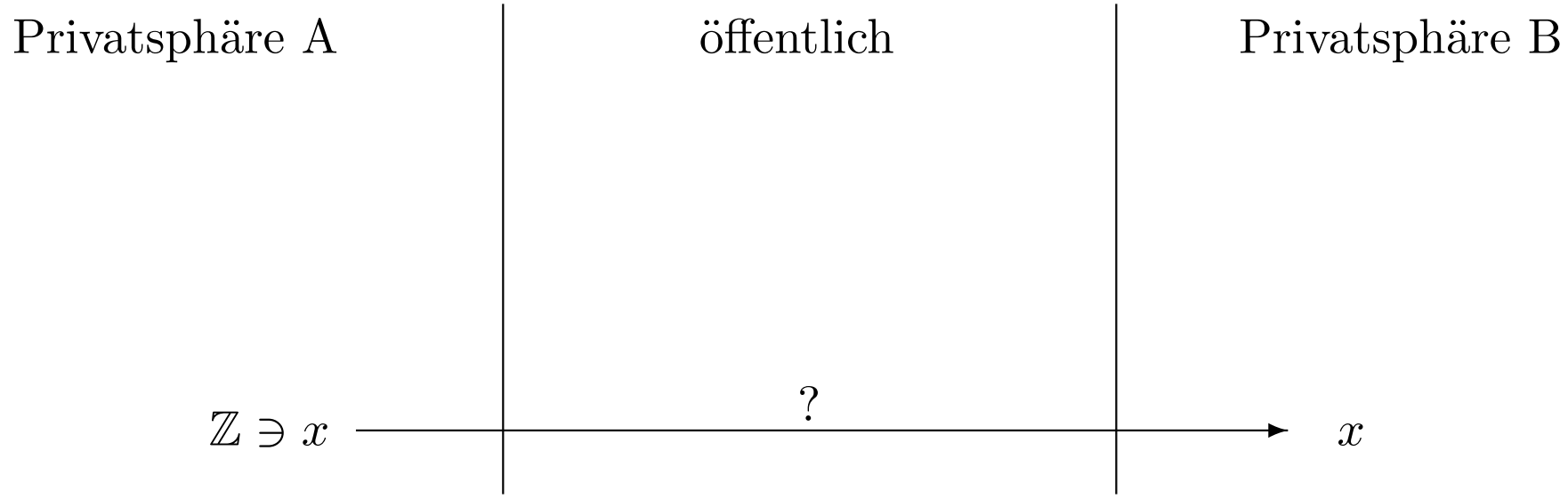

069 / 490101
LB DX 686


06
D
S 12
Ahrstraße
45


COMITE INTERNATIONAL OLYMPIQUE

Verschlüsselung

Problem: A will eine Nachricht geheim an B senden



RSA-Verfahren

$p \neq q$ Primzahlen, $N = pq$, $\varphi(N) = (p-1)(q-1)$

Dann gilt:

$$x^{1+k\varphi(N)} \equiv x \pmod{N} \qquad \forall k \geq 0, \forall x \in \mathbb{Z}$$

RSA-Verfahren

$p \neq q$ Primzahlen, $N = pq$, $\varphi(N) = (p-1)(q-1)$

Dann gilt:

$$x^{1+k\varphi(N)} \equiv x \pmod{N} \qquad \forall k \geq 0, \forall x \in \mathbb{Z}$$

Für $d, e \in \mathbb{Z}$ mit $de = 1 + k\varphi(N)$ gilt:

$$(x^e)^d \equiv x \pmod{N} \quad \forall x \in \mathbb{Z}$$

Genauer:

- wähle $e \in \mathbb{Z}$ mit $\mathrm{ggT}(e, \varphi(N)) = 1$
- berechne $d \equiv e^{-1} \pmod{\varphi N}$

RSA-Verfahren

Privatsphäre A	öffentlich	Privatsphäre B
		p, q, e wählen

RSA-Verfahren

Privatsphäre A	öffentlich	Privatsphäre B
		p, q, e wählen
		$N = pq, d$ berechnen

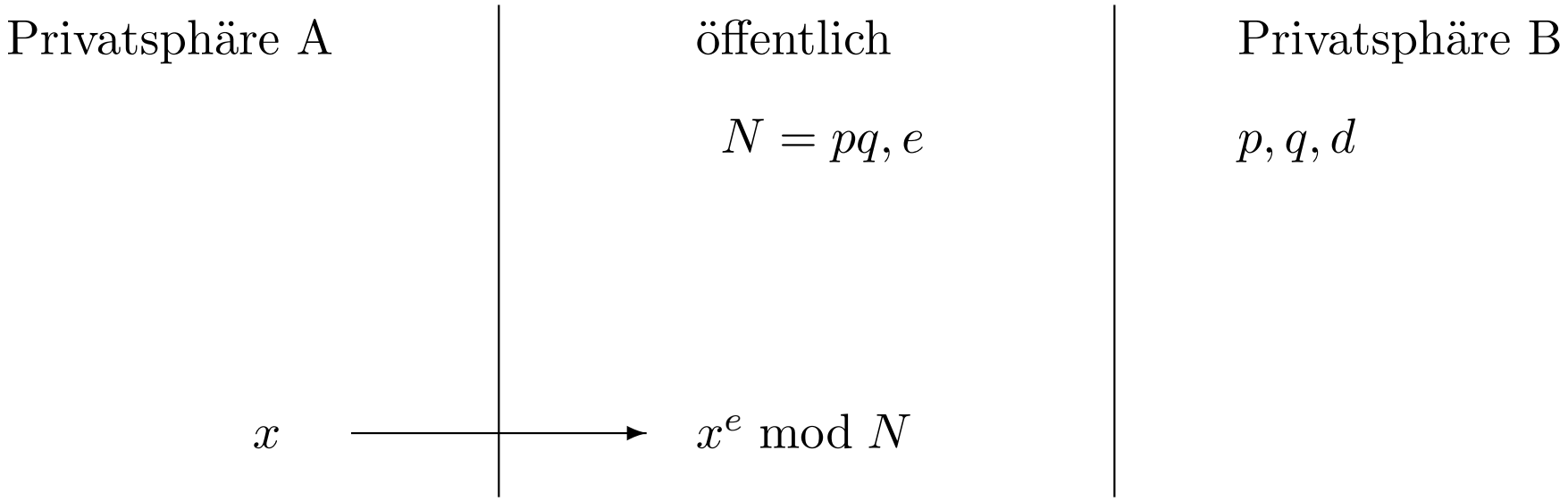
RSA-Verfahren

Privatsphäre A	öffentlich	Privatsphäre B
	$N = pq, e$	p, q, d

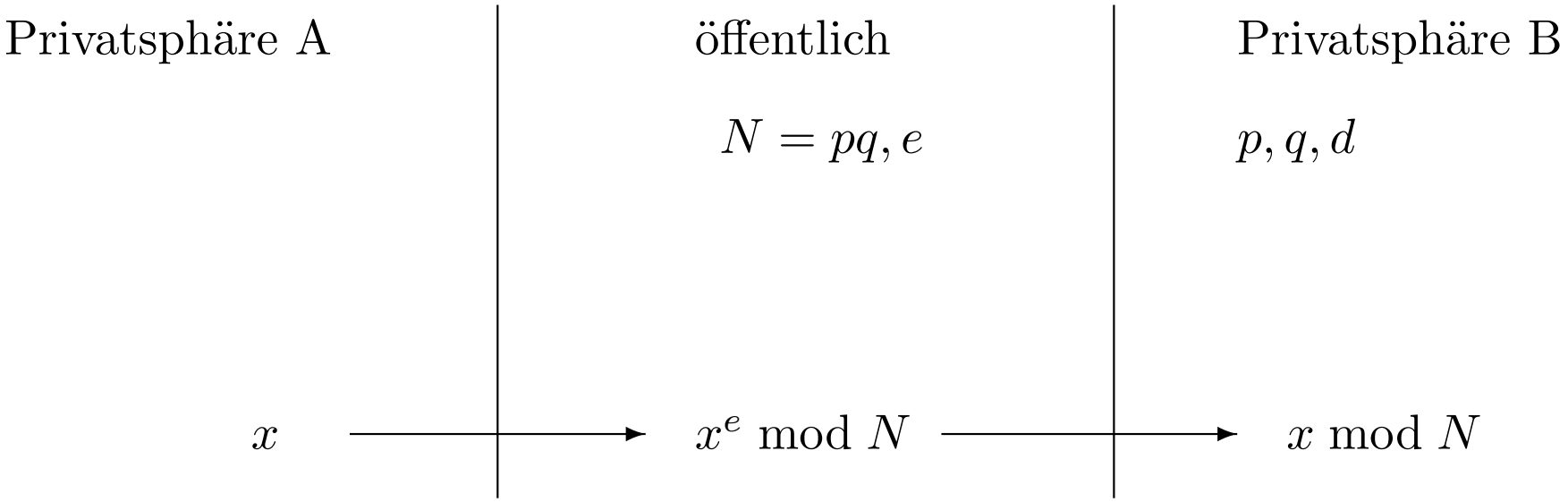
RSA-Verfahren

Privatsphäre A	öffentlich	Privatsphäre B
	$N = pq, e$	p, q, d
x		

RSA-Verfahren



RSA-Verfahren



Wieso ist das sicher?

Problem: Aus N, e, x^e mod N wieder x mod N berechnen!

Eine Möglichkeit:

N faktorisieren (schwer) $\Rightarrow p, q$ bekannt $\Rightarrow \varphi(N)$, d bekannt

Gibt es andere Möglichkeiten? Offenes Problem.

Faktorisieren

Satz 1 (Eindeutigkeit der Primfaktorzerlegung) *Jede natürliche Zahl $n > 0$ kann eindeutig in der Form*

$$n = p_1^{e_1} \cdot \ldots \cdot p_m^{e_m} \qquad m \geq 0, e_i > 0$$

dargestellt werden, wobei $p_1 < \ldots < p_m$ Primzahlen sind.

Problem: gegeben $N > 0$, finde diese Zerlegung

- oBdA: N keine Primzahlpotenz
- es reicht, echten Teiler von N zu finden

Das quadratische Sieb

Idee: finde (auf zufällige Art) x und y mit $x^2 \equiv y^2 \pmod{N}$

Das quadratische Sieb

Idee: finde (auf zufällige Art) x und y mit $x^2 \equiv y^2 \pmod{N}$

$N \mid x^2 - y^2 = (x+y)(x-y)$

$\mathrm{ggT}(x+y, N) \mid N$ echter Teiler mit Wahrscheinlichkeit $\geq \frac{1}{2}$, wenn N keine Primzahlpotenz ist (und $\mathrm{ggT}(N, xy) = 1$)

(z. B.: $N = pq$, $2 < p < q$

Lösungen mit $x \equiv \pm y \pmod{N}$ liefern keinen echten Teiler

Lösungen mit $x \equiv \pm y \pmod{p}$, $x \equiv \mp y \pmod{q}$ liefern echten Teiler)

Das quadratische Sieb

Idee: finde (auf zufällige Art) x und y mit $x^2 \equiv y^2 \pmod{N}$

1. solange x zufällig wählen, bis $x^2 \equiv 1$ gilt

Das quadratische Sieb

Idee: finde (auf zufällige Art) x und y mit $x^2 \equiv y^2 \pmod{N}$

1. solange x zufällig wählen, bis $x^2 \equiv 1$ gilt

2. auch gut:

$x_1^2 \equiv 150 = 2 \cdot 3 \cdot 5^2$

$x_2^2 \equiv 753 = 3 \cdot 251$

$x_3^2 \equiv 2008 = 2^3 \cdot 251$

Das quadratische Sieb

Idee: finde (auf zufällige Art) x und y mit $x^2 \equiv y^2 \pmod{N}$

1. solange x zufällig wählen, bis $x^2 \equiv 1$ gilt

2. auch gut:

$$x_1^2 \equiv 150 = 2 \cdot 3 \cdot 5^2$$
$$x_2^2 \equiv 753 = 3 \cdot 251 \qquad \Rightarrow \qquad (x_1 x_2 x_3)^2 \equiv (2^2 \cdot 3 \cdot 251)^2$$
$$x_3^2 \equiv 2008 = 2^3 \cdot 251$$

Das quadratische Sieb

Idee: finde (auf zufällige Art) x und y mit $x^2 \equiv y^2 \pmod{N}$

3. besser:

(a) $\mathcal{F} = \{p_1 = 2, p_2 = 3, \ldots, p_k\}$ erste k Primzahlen
($\mathcal{F}$ Faktorbasis)

Das quadratische Sieb

Idee: finde (auf zufällige Art) x und y mit $x^2 \equiv y^2 \pmod{N}$

3. besser:

(a) $\mathcal{F} = \{p_1 = 2, p_2 = 3, \ldots, p_k\}$ erste k Primzahlen
($\mathcal{F}$ Faktorbasis)

(b) suche $x_i^2 \equiv r_i$ (r_i Produkt von Primzahlen aus $\mathcal{F}$)

Das quadratische Sieb

Idee: finde (auf zufällige Art) x und y mit $x^2 \equiv y^2 \pmod{N}$

3. besser:

(a) $\mathcal{F} = \{p_1 = 2, p_2 = 3, \ldots, p_k\}$ erste k Primzahlen
($\mathcal{F}$ Faktorbasis)

(b) suche $x_i^2 \equiv r_i$ (r_i Produkt von Primzahlen aus $\mathcal{F}$)

(c) ab $k+1$ Kongruenzen in (b): finden I mit

$$\Big(\prod_{i \in I} x_i\Big)^2 \equiv \prod_{i \in I} r_i \equiv (\ldots)^2$$

(Gaußelimination)

Warum klappt das?

Satz 2 (Canfield, Erdös, Pomerance)

Sei $\psi(x,y) = \#\{n \leq x | n \text{ zerfällt in Primzahlen} \leq y\}$.
Für $\epsilon > 0$ *und* $3 \leq u \leq (1-\epsilon)\frac{\log x}{\log\log x}$ *gilt*

$$\psi(x, x^{\frac{1}{u}}) = xu^{-u(1+R)}$$

mit $|R| < c_\epsilon \frac{\log\log u}{\log u}$, *wobei die Konstante* c_ϵ *nur von* ϵ *abhängt.*

Umformulierung: Für eine Zahl z ist die Wahrscheinlichkeit, alle Primfaktoren kleiner als z^v, $v < 1$ zu haben, etwa $v^{\frac{1}{v}}$.

Warum klappt das?

Umformulierung: Für eine Zahl z ist die Wahrscheinlichkeit, alle Primfaktoren kleiner als z^v, $v < 1$ zu haben, etwa $v^{\frac{1}{v}}$.

Z. B.: Wähle $k = e^{\sqrt{\log N \log\log N}}$, also $p_k > e^{\sqrt{\log N \log\log N}}$

Wahrscheinlichkeit eine Kongruenz zu finden: $\approx e^{-\frac{1}{2}\sqrt{\log N \log\log N}}$

$\Rightarrow$ haben nach etwa $e^{\frac{3}{2}\sqrt{\log N \log\log N}}$ Versuchen genügend viele Kongruenzen

$e^{\frac{3}{2}\sqrt{\log N \log\log N}}$ ist VIEL kleiner als N oder $\sqrt{N}$

Das Zahlkörpersieb am Beispiel einer speziellen Zahl

$N = 2^{1039} - 1$

Das Zahlkörpersieb am Beispiel einer speziellen Zahl

$N = 2^{1039} - 1$

$$32N = 2^{1044} - 32 = (2^{174})^6 - (\sqrt[6]{32})^6 = (2^{174} - \sqrt[6]{32}) \cdot (2^{5 \cdot 174} + \cdots + \sqrt[6]{32}^5)$$

Das Zahlkörpersieb am Beispiel einer speziellen Zahl

$N = 2^{1039} - 1$

$$32N = 2^{1044} - 32 = (2^{174})^6 - (\sqrt[6]{32})^6 = (2^{174} - \sqrt[6]{32}) \cdot (2^{5 \cdot 174} + \cdots + \sqrt[6]{32}^5)$$

Zerlege $2^{174} - \sqrt[6]{32}$

$\Rightarrow$ Betrachte den Ring $R = \mathbb{Z}[\sqrt[6]{2}]$

Einschub über $R = \mathbb{Z}[\sqrt[6]{2}]$

Definition:

$$R = \left\{ a + b\sqrt[6]{2} + c\sqrt[6]{4} + d\sqrt[6]{8} + e\sqrt[6]{16} + f\sqrt[6]{32} \;\middle|\; a, b, c, d, e, f \in \mathbb{Z} \right\}$$

Eigenschaften:

1. wir können in R addieren, subtrahieren, multiplizieren
2. Teilbarkeit $(0 \neq \alpha \mid \beta \Leftrightarrow \exists \gamma \in R \text{ mit } \alpha\gamma = \beta)$
3. Kongruenzen $(\alpha \equiv \beta \pmod{\gamma}, \gamma \neq 0 \Leftrightarrow \gamma \mid \alpha - \beta)$

Einschub über $R = \mathbb{Z}[\sqrt[6]{2}]$

Definition:

$$R = \left\{ a + b\sqrt[6]{2} + c\sqrt[6]{4} + d\sqrt[6]{8} + e\sqrt[6]{16} + f\sqrt[6]{32} \;\middle|\; a, b, c, d, e, f \in \mathbb{Z} \right\}$$

Satz 3 *Nach Wahl von Primelementen* $\pi_1, \pi_2, \ldots$ *kann jedes* $0 \neq \alpha \in R$ *eindeutig als*

$$\alpha = \pm \epsilon_1^{a_1} \epsilon_2^{a_2} \epsilon_3^{a_3} \cdot \pi_{i_1}^{e_1} \cdot \ldots \cdot \pi_{i_m}^{e_m} \qquad m \geq 0, e_i > 0, a_i \in \mathbb{Z}$$

dargestellt werden, wobei
$\epsilon_1 = 1 + \sqrt[6]{8}, \epsilon_2 = 1 + \sqrt[6]{2} + \sqrt[6]{4}, \epsilon_3 = 1 - \sqrt[6]{2} + \sqrt[6]{4}$ *ist.*

Fazit: Wir können im wesentlichen in R genauso wie in $\mathbb{Z}$ rechnen.

Achtung: Der Satz gilt nicht immer, z. B. bei $\mathbb{Z}[\sqrt[6]{2008}]$.

Das Zahlkörpersieb am Beispiel einer speziellen Zahl

$N = 2^{1039} - 1$

$$32N = 2^{1044} - 32 = (2^{174})^6 - (\sqrt[6]{32})^6 = (2^{174} - \sqrt[6]{32}) \cdot (2^{5 \cdot 174} + \cdots + \sqrt[6]{32}^5)$$

Zerlege $2^{174} - \sqrt[6]{32}$

Das Zahlkörpersieb am Beispiel einer speziellen Zahl

$N = 2^{1039} - 1$

$$32N = 2^{1044} - 32 = (2^{174})^6 - (\sqrt[6]{32})^6 = (2^{174} - \sqrt[6]{32}) \cdot (2^{5 \cdot 174} + \cdots + \sqrt[6]{32}^5)$$

Zerlege $2^{174} - \sqrt[6]{32}$

echter Teiler von $2^{174} - \sqrt[6]{32}$ liefert echten Teiler von N

- Restklassen modulo $2^{174} - \sqrt[6]{32}$ lassen sich durch $0, 1, \ldots, N-1$ repräsentieren
- Teiler τ von $2^{174} - \sqrt[6]{32}$ werde durch t repräsentiert
- τ echter Teiler von $2^{174} - \sqrt[6]{32} \Rightarrow t$ echter Teiler von N

Zerlegung von $2^{174} - \sqrt[6]{32}$

Betrachte

$$a - b \cdot 2^{174} \equiv a - b\sqrt[6]{32} \pmod{2^{174} - \sqrt[6]{32}} \qquad a, b \in \mathbb{Z}$$

Zerlegung von $2^{174} - \sqrt[6]{32}$

Betrachte

$$\underbrace{a - b \cdot 2^{174}}_{\text{in } \mathbb{Z} \text{ faktorisieren}} \equiv \underbrace{a - b\sqrt[6]{32}}_{\text{in } R \text{ faktorisieren}} \pmod{2^{174} - \sqrt[6]{32}} \qquad a, b \in \mathbb{Z}$$

Zerlegung von $2^{174} - \sqrt[6]{32}$

Betrachte

$$\underbrace{a - b \cdot 2^{174}}_{\text{in } \mathbb{Z} \text{ faktorisieren}} \equiv \underbrace{a - b\sqrt[6]{32}}_{\text{in } R \text{ faktorisieren}} \pmod{2^{174} - \sqrt[6]{32}} \qquad a, b \in \mathbb{Z}$$

$$p_1^{e_1} \cdot \ldots \cdot p_m^{e_m} \equiv \pm \epsilon_1^{a_1} \epsilon_2^{a_2} \epsilon_3^{a_3} \cdot \pi_{i_1}^{f_1} \cdot \ldots \cdot \pi_{i_n}^{f_n} \pmod{2^{174} - \sqrt[6]{32}}$$

Zerlegung von $2^{174} - \sqrt[6]{32}$

Betrachte

$$\underbrace{a - b \cdot 2^{174}}_{\text{in } \mathbb{Z} \text{ faktorisieren}} \equiv \underbrace{a - b\sqrt[6]{32}}_{\text{in } R \text{ faktorisieren}} \pmod{2^{174} - \sqrt[6]{32}} \qquad a, b \in \mathbb{Z}$$

$$p_1^{e_1} \cdot \ldots \cdot p_m^{e_m} \equiv \pm \epsilon_1^{a_1} \epsilon_2^{a_2} \epsilon_3^{a_3} \cdot \pi_{i_1}^{f_1} \cdot \ldots \cdot \pi_{i_n}^{f_n} \pmod{2^{174} - \sqrt[6]{32}}$$

Rest im wesentlichen wie bisher:

- wenn beide Seiten in „kleine Primzahlen“ zerfallen $\Rightarrow$ Kongruenz
- mehr Kongruenzen als Faktorbasiselemente sammeln
- $\Rightarrow \alpha^2 \equiv \beta^2 \pmod{2^{174} - \sqrt[6]{32}}$, also echten Teiler mit Wahrscheinlichkeit $\geq \frac{1}{2}$

Ergebnis

$$2^{1039} - 1 = 5080711 \times$$

$$55853666619936291260749204658315944968646527018488637648010052346319853288374753 \times$$

$$20758181946442382764570481370359469516293970800739520988120838703792729090324679382343143884144834882534053344769112223028158327696525376091410189105241993899334109711624358962065972167481161749004803659735573409253205425523689$$