

Algebry a šifry

Jak přenést tajemství?

Martin Rosenberg¹

Seminář algebry, GNA, 2026

¹martin.rosenberg@alej.cz

Situace

- **Alice** a **Bob** si chtějí poslat zprávu tak, aby **Eva** nedokázala přečíst její obsah
 - Komunikace mezi Alicí a Bobem je veřejná
 - ⇒ Eva dokáže přečíst vše

Situace

- **Alice** a **Bob** si chtějí poslat zprávu tak, aby **Eva** nedokázala přečíst její obsah
 - Komunikace mezi Alicí a Bobem je veřejná
 - ⇒ Eva dokáže přečíst vše

Pokud Eva vidí vše, mohou Alice a Bob bezpečně komunikovat?
Mohou se Alice a Bob dohodnout na tajemství, i když je každá zpráva viditelná?

Situace

- Mohou se potkat osobně

Situace

- Mohou se potkat osobně
⇒ nepraktické

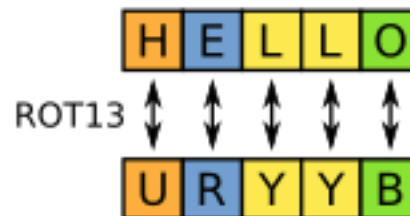
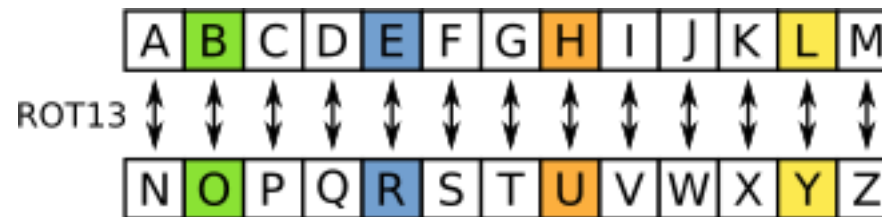
Situace

- Mohou se potkat osobně
⇒ nepraktické
- Komunikace na internetu
- Šifrování zpráv na papíře (WWII)

Šifry

Caesarova šifra (1. stol. př. n. l.)

- Substituční šifra
- Vezmu zprávu a každé písmeno nahradím písmenem jiným (posunutým)
- Posun o k , šifra $c = (m + k) \bmod 26$



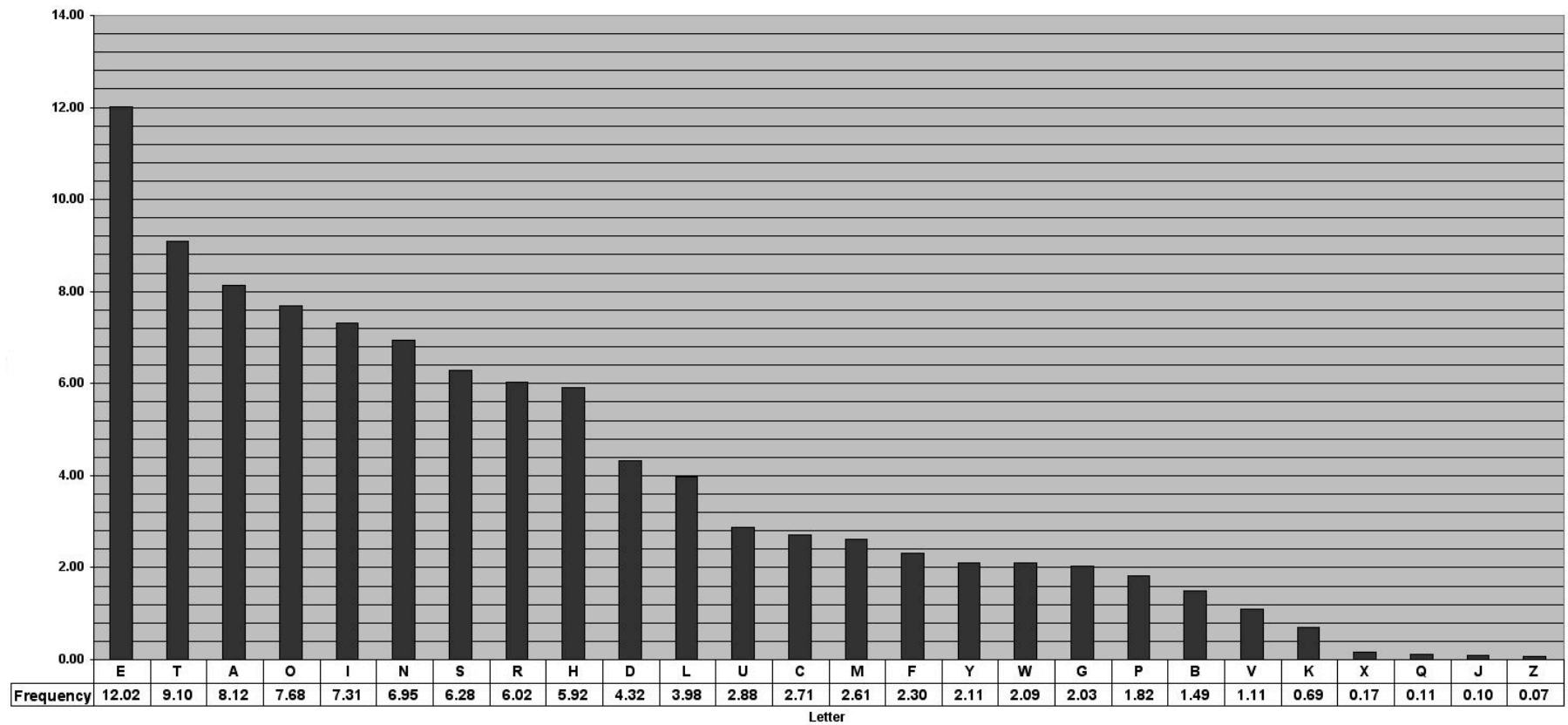
Caesarova šifra (1. stol. př. n. l.)

Pokuste se rozluštit

KH00R ZRU0G

Útoky na CŠ

- Frekvenční analýza



Vigenèrova šifra (Bellaso 1553, Vigenère 1586)

- Polyalfabetická substituční šifra
- Vícekrát použitá Caesarova šifra
- Výhoda: jedno písmeno se může zašifrovat vícero způsoby
- Máme text a **klíč**, podle písmen pod sebou vyhledáme zašifrované písmeno
- Ve své době označovaná za **neprolomitelnou**

Vigenèrova šifra (Bellaso 1553, Vigenère 1586)

- Polyalfabetická substituční šifra
- Vícekrát použitá Caesarova šifra
- Výhoda: jedno písmeno se může zašifrovat vícero způsoby
- Máme text a **klíč**, podle písmen pod sebou vyhledáme zašifrované písmeno
- Ve své době označovaná za **neprolomitelnou**
 - ▶ 1863 Kasiskiho test

Vigenèrova šifra (Bellaso 1553, Vigenère 1586)

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

XOR (Exkluzivní disjunkce)

a	b	$a \oplus b$
0	0	0
0	1	1
1	0	1
1	1	0

- Jako disjunkce až na poslední řádek
- Pěkné vlastnosti

XOR (Exkluzivní disjunkce)

a	b	$a \oplus b$
0	0	0
0	1	1
1	0	1
1	1	0

- Jako disjunkce až na poslední řádek
- Pěkné vlastnosti
 - Sám sobě inverzní: $a \oplus b = c \Rightarrow c \oplus b = a$

XOR (Exkluzivní disjunkce)

a	b	$a \oplus b$
0	0	0
0	1	1
1	0	1
1	1	0

- Jako disjunkce až na poslední řádek
- Pěkné vlastnosti
 - Sám sobě inverzní: $a \oplus b = c \Rightarrow c \oplus b = a$
 - Pro zafixované a je $a \oplus b$ uniformně rozdělené

XOR (Exkluzivní disjunkce)

a	b	$a \oplus b$
0	0	0
0	1	1
1	0	1
1	1	0

- Jako disjunkce až na poslední řádek
- Pěkné vlastnosti
 - Sám sobě inverzní: $a \oplus b = c \Rightarrow c \oplus b = a$
 - Pro zafixované a je $a \oplus b$ uniformně rozdělené
 - Sčítání ve dvojkové soustavě

One-time pad

- **Klíč** je uniformně náhodný, stejně dlouhý jako zpráva
- Zašifrování: $c = m \oplus k$

One-time pad

- **Klíč** je uniformně náhodný, stejně dlouhý jako zpráva
- Zašifrování: $c = m \oplus k$
- Odšifrování: $m = c \oplus k$

One-time pad

- **Klíč** je uniformně náhodný, stejně dlouhý jako zpráva
- Zašifrování: $c = m \oplus k$
- Odšifrování: $m = c \oplus k$
- Pokud je klíč **skutečně náhodný** a **použitý pouze jednou**, je šifrový text absolutně bezpečný

One-time pad

- **Klíč** je uniformně náhodný, stejně dlouhý jako zpráva
- Zašifrování: $c = m \oplus k$
- Odšifrování: $m = c \oplus k$
- Pokud je klíč **skutečně náhodný** a **použitý pouze jednou**, je šifrový text absolutně bezpečný
 - ▶ 1949 Shannon dokázal, že OTP je absolutně bezpečný
 - ▶ Eva zná jen délku zprávy
 - ▶ Verona project (WWII): Američtí kryptoanalytici dešifrovali sovětské OTP, protože opakovali klíče

One-time pad

- Klíč musí být
 - náhodný
 - stejně dlouhý jako zpráva
 - jednorázový

One-time pad

- Klíč musí být
 - náhodný
 - stejně dlouhý jako zpráva
 - jednorázový
- Jak může **Alice** s **Bobem** klíč nasdílet?

One-time pad

- Klíč musí být
 - náhodný
 - stejně dlouhý jako zpráva
 - jednorázový
- Jak může **Alice** s **Bobem** klíč nasdílet?
 - předat osobně?

One-time pad

- Klíč musí být
 - náhodný
 - stejně dlouhý jako zpráva
 - jednorázový
- Jak může **Alice** s **Bobem** klíč nasdílet?
 - předat osobně?
 - poslat, ale to ho může vidět Eva (slepice a vejce)

Kerckhoffsův princip

**Bezpečnost kryptografického systému
by měla záviset **pouze** na utajení klíče**

- Žádná *security by obscurity*
 - Algoritmy šifer jsou veřejné

Modulární aritmetika

Co to je

- Hodinová aritmetika, počítání se zbytky
 - Výsledky „přetékaají“ zpět
- Slovíčko mod

Co to je

- Hodinová aritmetika, počítání se zbytky
 - Výsledky „přetékaají“ zpět
- Slovíčko mod
- $17 \bmod 12 = ?$

Co to je

- Hodinová aritmetika, počítání se zbytky
 - Výsledky „přetékaají“ zpět
- Slovíčko mod
- $17 \bmod 12 = ?$

Výsledek je zbytek po dělení.
To je všechno.

Co to je

Vypočítejte

$$7^4 \equiv ? \pmod{13}$$

$$7^{12} \equiv ? \pmod{13}$$

Prvočísla

- Mějme prvočíslo p
 - Pak $\{1, 2, 3, \dots, p - 1\}$ tvoří multiplikatívni grupu \mathbb{Z}_p^*

Prvočísla

- Mějme prvočíslo p
 - Pak $\{1, 2, 3, \dots, p - 1\}$ tvoří multiplikatívni grupu \mathbb{Z}_p^*
 - Každý prvek má inverzní prvek: $a \cdot a^{-1} \equiv 1 \pmod{p}$

Prvočísla

- Mějme prvočíslo p
 - Pak $\{1, 2, 3, \dots, p - 1\}$ tvoří multiplikativní grupu \mathbb{Z}_p^*
 - Každý prvek má inverzní prvek: $a \cdot a^{-1} \equiv 1 \pmod{p}$
- Prvek g je *generátor*, pokud mocniny g tvoří všechny prvky \mathbb{Z}_p^*

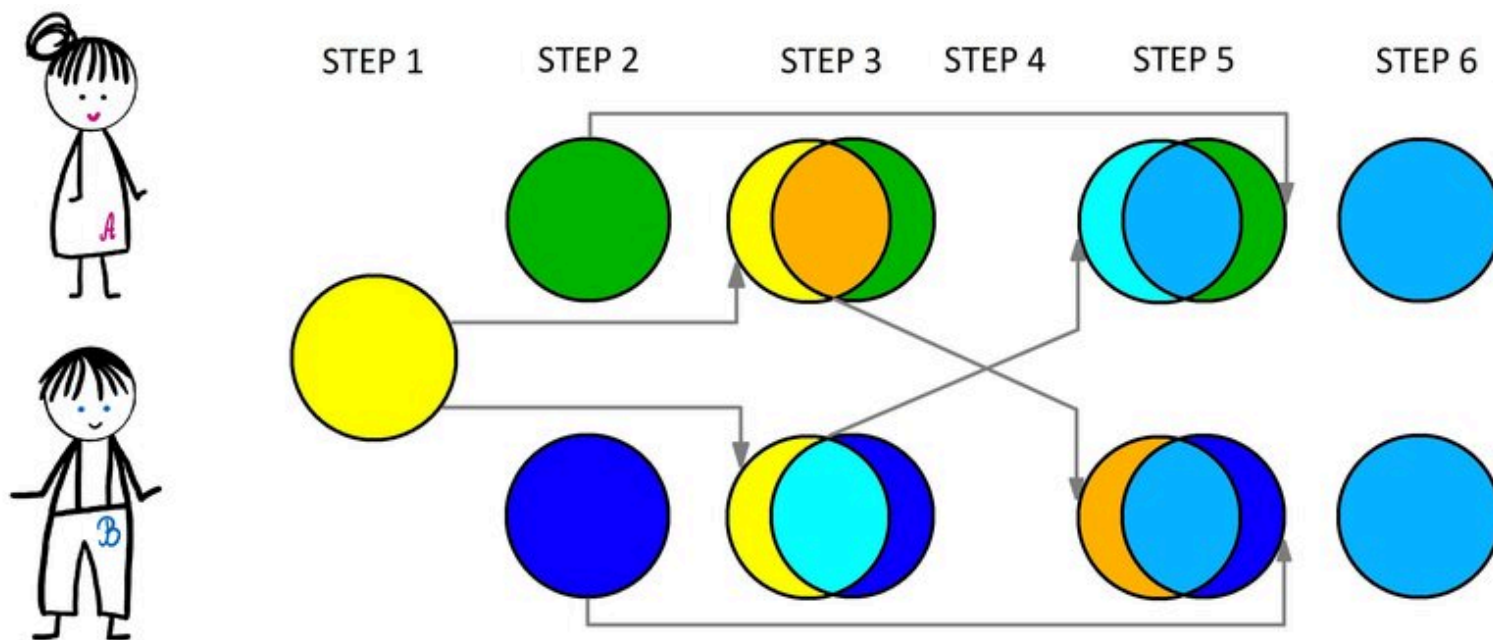
Domluva

- Alice se s Bobem potřebuje domluvit na tajemství
 - Třeba na klíči k nějaké šifře

Domluva

- Alice se s Bobem potřebuje domluvit na tajemství
 - Třeba na klíči k nějaké šifře
- Musí to udělat po **nezabezpečeném** kanálu
 - Eva čte vše

Diffie-Hellmannova výměna klíčů



Diffieho-Hellmannova výměna klíčů

1. Oba znají (nemusí být tajné): prvočíslo p , generátor g

Diffieho-Hellmannova výměna klíčů

1. Oba znají (nemusí být tajné): prvočíslo p , generátor g
2. Alice zvolí tajné a , vypočte $A = g^a \bmod p$

Diffieho-Hellmannova výměna klíčů

1. Oba znají (nemusí být tajné): prvočíslo p , generátor g
2. Alice zvolí tajné a , vypočte $A = g^a \bmod p$
3. Bob zvolí tajné b , vypočte $B = g^b \bmod p$

Diffieho-Hellmannova výměna klíčů

1. Oba znají (nemusí být tajné): prvočíslo p , generátor g
2. Alice zvolí tajné a , vypočte $A = g^a \bmod p$
3. Bob zvolí tajné b , vypočte $B = g^b \bmod p$
4. **Vymění** si A a B

Diffieho-Hellmannova výměna klíčů

1. Oba znají (nemusí být tajné): prvočíslo p , generátor g
2. Alice zvolí tajné a , vypočte $A = g^a \bmod p$
3. Bob zvolí tajné b , vypočte $B = g^b \bmod p$
4. **Vymění** si A a B
5. Alice vypočte $B^a \bmod p = g^{ba} \bmod p = k$

Diffieho-Hellmannova výměna klíčů

1. Oba znají (nemusí být tajné): prvočíslo p , generátor g
2. Alice zvolí tajné a , vypočte $A = g^a \bmod p$
3. Bob zvolí tajné b , vypočte $B = g^b \bmod p$
4. **Vymění** si A a B
5. Alice vypočte $B^a \bmod p = g^{ba} \bmod p = k$
 1. Bob vypočte $A^b \bmod p = g^{ab} \bmod p = k$

Stejný výsledek!

Diffieho-Hellmannova výměna klíčů

1. Oba znají (nemusí být tajné): prvočíslo p , generátor g
2. Alice zvolí tajné a , vypočte $A = g^a \bmod p$
3. Bob zvolí tajné b , vypočte $B = g^b \bmod p$
4. **Vymění** si A a B
5. Alice vypočte $B^a \bmod p = g^{ba} \bmod p = k$
 1. Bob vypočte $A^b \bmod p = g^{ab} \bmod p = k$

Stejný výsledek!

- Eva zná jen g, p, A, B . Aby vypočetla k , musela by znát a nebo b

Proč DHKE funguje?

- Eva by potřebovala z $g, p, A = g^a \pmod{p}$ najít a

Proč DHKE funguje?

- Eva by potřebovala z $g, p, A = g^a \pmod p$ najít a
- Chtěli bychom něco jako *inverzní funkci* k mocnění v \mathbb{Z}_p^*

Proč DHKE funguje?

Vyřešte

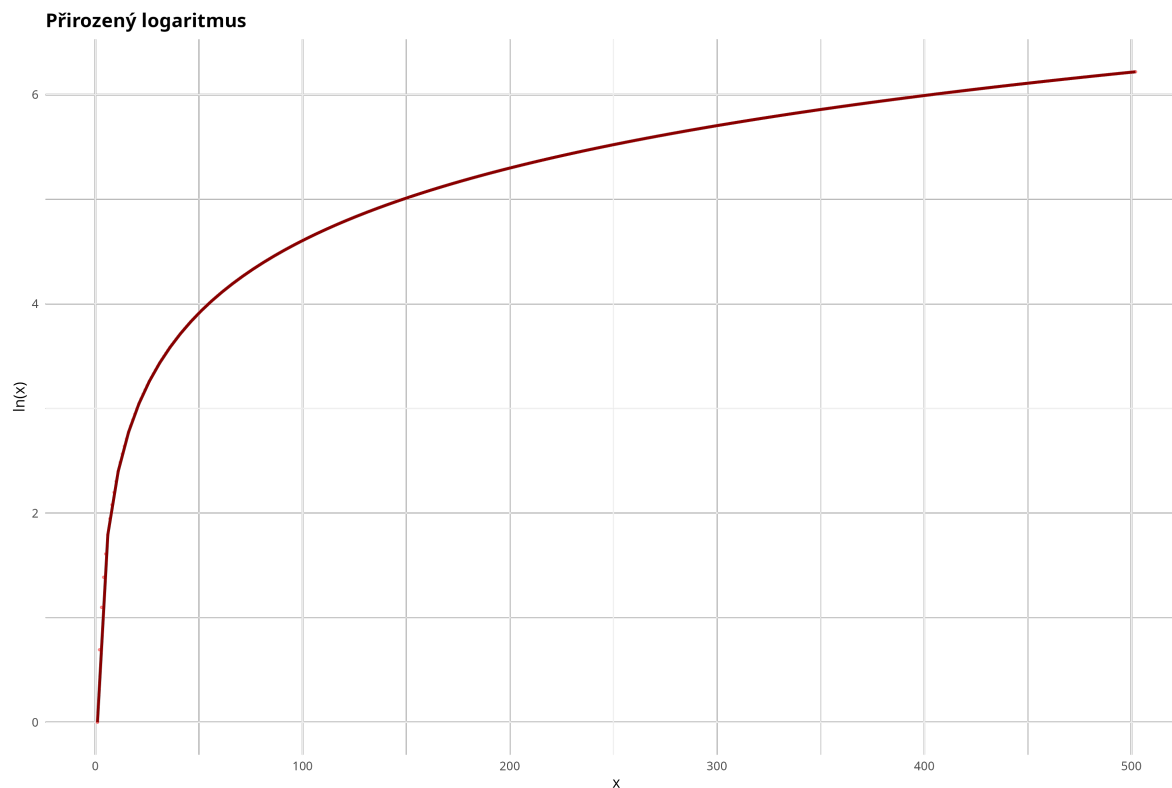
$$5^? \equiv 8 \pmod{23}$$

Problém diskrétního logaritmu

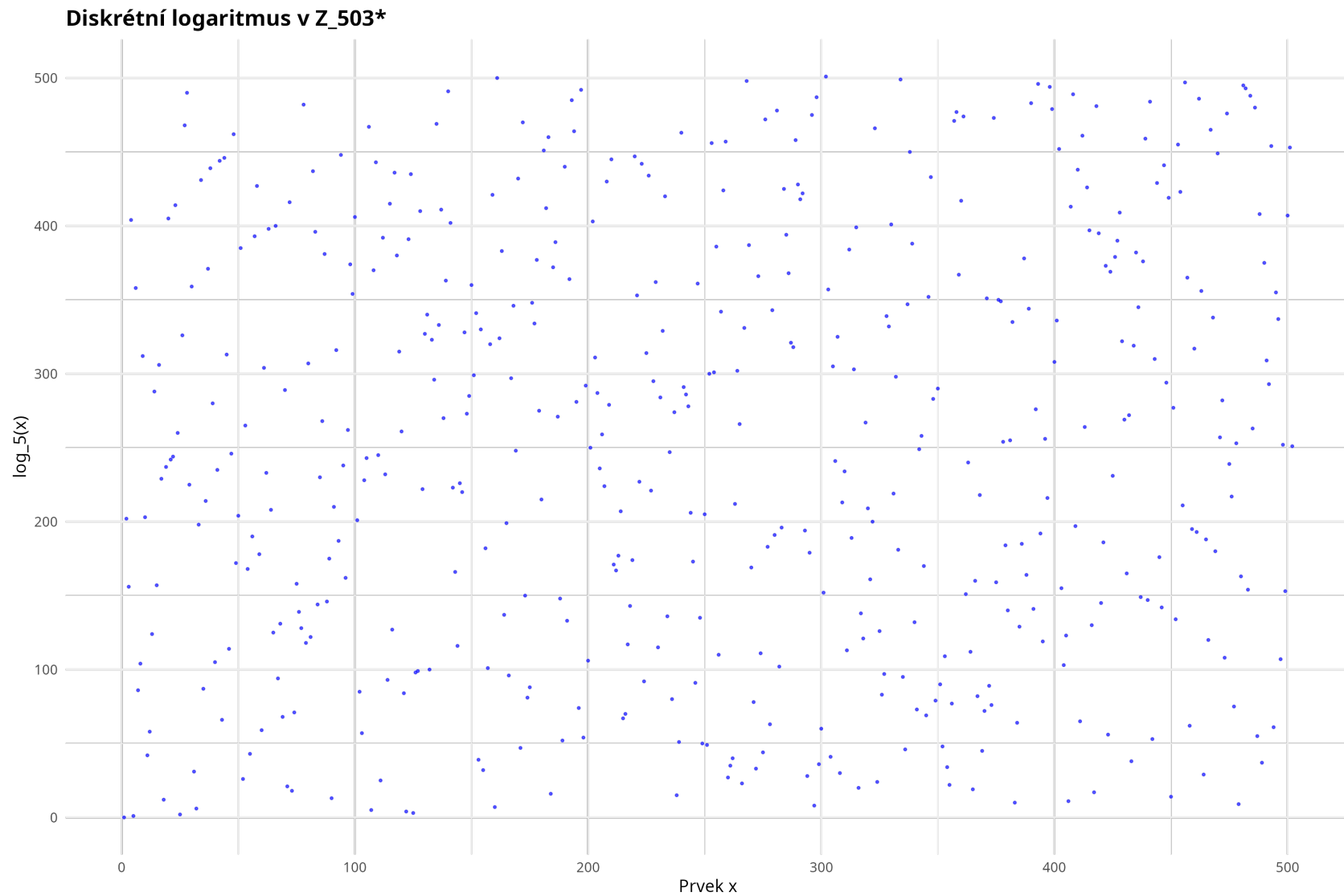
- V reálných číslech je logaritmus monotónní, rostoucí, předvídatelný

Problém diskrétního logaritmu

- V reálných číslech je logaritmus monotónní, rostoucí, předvídatelný



Problém diskrétního logaritmu



Problém diskretního logaritmu

- Nejrychlejší algoritmy na výpočet diskretního logaritmu jsou velmi pomalé

Problém diskretního logaritmu

- Nejrychlejší algoritmy na výpočet diskretního logaritmu jsou velmi pomalé
- Nevíme, jestli existuje rychlejší algoritmus

Faktorzace

Faktorizace (rozklad na prvočísla)

- Vynásobení dvou velkých prvočísel $p \cdot q = n$ je jednoduché a okamžité

Faktorizace (rozklad na prvočísla)

- Vynásobení dvou velkých prvočísel $p \cdot q = n$ je jednoduché a okamžité
- Rozložit n na p a q je složité (algoritmicky velmi pomalé)

Faktorizace (rozklad na prvočísla)

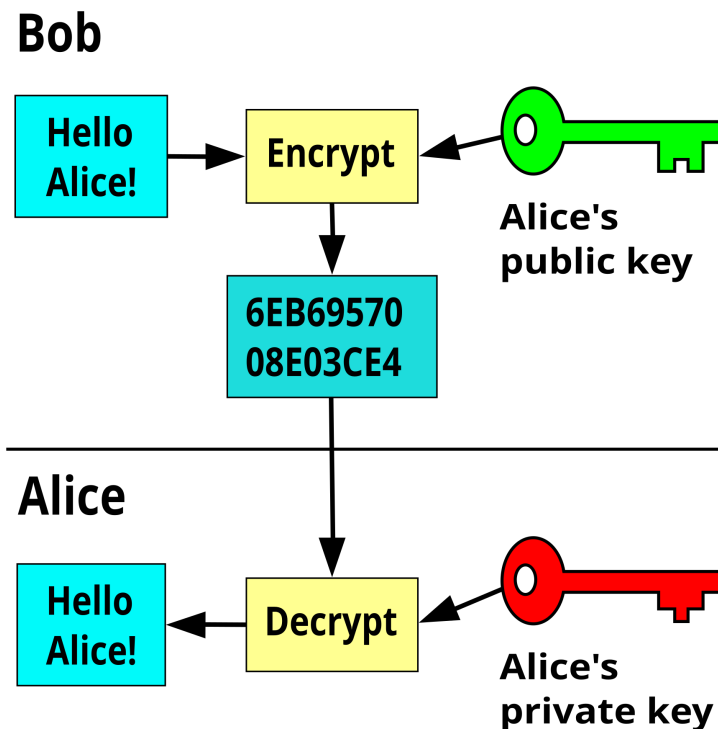
- Vynásobení dvou velkých prvočísel $p \cdot q = n$ je jednoduché a okamžité
- Rozložit n na p a q je složité (algoritmicky velmi pomalé)
- Analogie problému diskrétního logaritmu (one-way)
- Problém rozkladu využitý v šifrách, např. RSA

RSA

- 1977, Rivest-Shamir-Adleman
- Asymetrická šifra
 - **Veřejný** klíč slouží k šifrování zpráv adresátovi
 - **Soukromý** klíč slouží k dešifrování adresátem

RSA

- 1977, Rivest-Shamir-Adleman
- Asymetrická šifra
 - **Veřejný** klíč slouží k šifrování zpráv adresátovi
 - **Soukromý** klíč slouží k dešifrování adresátem



Pan Euler

- Eulerova funkce $\varphi(n)$: počet všech čísel nesoudělných s n

¹Důkaz pomocí Čínské věty o zbytcích (CRT)

Pan Euler

- Eulerova funkce $\varphi(n)$: počet všech čísel nesoudělných s n
 - $\varphi(1) = 1$

¹Důkaz pomocí Čínské věty o zbytcích (CRT)

Pan Euler

- Eulerova funkce $\varphi(n)$: počet všech čísel nesoudělných s n
 - $\varphi(1) = 1$
 - $\varphi(p) = p - 1$ pro p prvočíslo

¹Důkaz pomocí Čínské věty o zbytcích (CRT)

Pan Euler

- Eulerova funkce $\varphi(n)$: počet všech čísel nesoudělných s n
 - $\varphi(1) = 1$
 - $\varphi(p) = p - 1$ pro p prvočíslo

Pro $n = p \cdot q$, kde p, q prvočísla platí¹

$$\varphi(n) = \varphi(p \cdot q) = (p - 1)(q - 1)$$

¹Důkaz pomocí Čínské věty o zbytcích (CRT)

Pan Euler

- Eulerova funkce $\varphi(n)$: počet všech čísel nesoudělných s n
 - $\varphi(1) = 1$
 - $\varphi(p) = p - 1$ pro p prvočíslo

Pro $n = p \cdot q$, kde p, q prvočísla platí¹

$$\varphi(n) = \varphi(p \cdot q) = (p - 1)(q - 1)$$

Znám-li n , vypočítat $\varphi(n)$ je stejně těžké, jako rozložit n na p a q .

¹Důkaz pomocí Čínské věty o zbytcích (CRT)

Pan Euler

- Pro n, m nesoudělné s n také platí

$$m^{\varphi(n)} \equiv 1 \pmod{n}$$

Pan Euler

- Pro n, m nesoudělné s n také platí

$$m^{\varphi(n)} \equiv 1 \pmod{n}$$

Ověřte pro $n = 7$ a $m = 3$

Pan Euler

- Pro n, m nesoudělné s n také platí

$$m^{\varphi(n)} \equiv 1 \pmod{n}$$

Ověřte pro $n = 7$ a $m = 3$

$$3^1 = 3, 3^2 = 2, 3^3 = 6$$

$$3^4 = 4, 3^5 = 5, 3^6 = 1$$

Pan Euler

- Pro n, m nesoudělné s n také platí

$$m^{\varphi(n)} \equiv 1 \pmod{n}$$

Ověřte pro $n = 7$ a $m = 3$

$$3^1 = 3, 3^2 = 2, 3^3 = 6$$

$$3^4 = 4, 3^5 = 5, 3^6 = 1$$

- Pro prvočíslo p a $m \in \mathbb{Z}_p^*$ platí $m^{p-1} \equiv 1 \pmod{p}$
 - Malá Fermatova věta

Volba klíčů

- Vybereme prvočísla p, q , spočteme n a $\varphi(n)$
- Vezmi e nesoudělné s $\varphi(n)$ ¹

¹Pro RSA je častá volba číslo 65537. Při volbě p a q ověřujeme, že jsou nesoudělná.

²Pomocí rozšířeného Eukleidova algoritmu

Volba klíčů

- Vybereme prvočísla p, q , spočteme n a $\varphi(n)$
- Vezmi e nesoudělné s $\varphi(n)$ ¹
 - Dvojice (n, e) tvoří **veřejný** klíč

¹Pro RSA je častá volba číslo 65537. Při volbě p a q ověřujeme, že jsou nesoudělná.

²Pomocí rozšířeného Eukleidova algoritmu

Volba klíčů

- Vybereme prvočísla p, q , spočteme n a $\varphi(n)$
- Vezmi e nesoudělné s $\varphi(n)$ ¹
 - Dvojice (n, e) tvoří **veřejný** klíč
- Najdi d tž. $e \cdot d \equiv 1 \pmod{\varphi(n)}$

¹Pro RSA je častá volba číslo 65537. Při volbě p a q ověřujeme, že jsou nesoudělná.

²Pomocí rozšířeného Eukleidova algoritmu

Volba klíčů

- Vybereme prvočísla p, q , spočteme n a $\varphi(n)$
- Vezmi e nesoudělné s $\varphi(n)$ ¹
 - Dvojice (n, e) tvoří **veřejný** klíč
- Najdi d tž. $e \cdot d \equiv 1 \pmod{\varphi(n)}$
 - Inverzní prvek k e , algoritmicky rychlé²

¹Pro RSA je častá volba číslo 65537. Při volbě p a q ověřujeme, že jsou nesoudělná.

²Pomocí rozšířeného Eukleidova algoritmu

Volba klíčů

- Vybereme prvočísla p, q , spočteme n a $\varphi(n)$
- Vezmi e nesoudělné s $\varphi(n)$ ¹
 - Dvojice (n, e) tvoří **veřejný** klíč
- Najdi d tž. $e \cdot d \equiv 1 \pmod{\varphi(n)}$
 - Inverzní prvek k e , algoritmicky rychlé²
 - Číslo d je **soukromý** klíč

¹Pro RSA je častá volba číslo 65537. Při volbě p a q ověřujeme, že jsou nesoudělná.

²Pomocí rozšířeného Eukleidova algoritmu

Zašifrování a dešifrování

- Alice chce Bobovi poslat písmeno A
 - Na počítačích kódováno jako číslo $m = 65$
- Vezme Bobův **veřejný** klíč (n, e) a spočte

$$c = m^e \bmod n$$

- Bob přijme zprávu c a použije svůj **soukromý** klíč

$$m = c^d \bmod n$$

Proč to funguje?

$$c^d = (m^e)^d = m^{ed} \equiv m \pmod{n}$$

Proč to funguje?

$$c^d = (m^e)^d = m^{ed} \equiv m \pmod{n}$$

Chceme ukázat, že platí

$$m^{ed} \equiv m \pmod{n}$$

Proč to funguje?

$$c^d = (m^e)^d = m^{ed} \equiv m \pmod{n}$$

Chceme ukázat, že platí

$$m^{ed} \equiv m \pmod{n}$$

Bob zvolil d tak, že $ed \equiv 1 \pmod{\varphi(n)}$

Proč to funguje?

$$c^d = (m^e)^d = m^{ed} \equiv m \pmod{n}$$

Chceme ukázat, že platí

$$m^{ed} \equiv m \pmod{n}$$

Bob zvolil d tak, že $ed \equiv 1 \pmod{\varphi(n)}$

$\Rightarrow ed = 1 + k \cdot \varphi(n)$ pro nějaké k

Proč to funguje?

$$c = m^{ed} \equiv m \pmod{n}$$

Proč to funguje?

$$c = m^{ed} \equiv m \pmod{n}$$
$$m^{ed} = m^{1+k \cdot \varphi(n)} =$$

Proč to funguje?

$$\begin{aligned}c &= m^{ed} \equiv m \pmod{n} \\m^{ed} &= m^{1+k \cdot \varphi(n)} = \\&= m^1 \cdot m^{k \cdot \varphi(n)} =\end{aligned}$$

Proč to funguje?

$$\begin{aligned}c &= m^{ed} \equiv m \pmod{n} \\m^{ed} &= m^{1+k \cdot \varphi(n)} = \\&= m^1 \cdot m^{k \cdot \varphi(n)} = \\&= m \cdot (m^{\varphi(n)})^k\end{aligned}$$

Proč to funguje?

$$\begin{aligned}c &= m^{ed} \equiv m \pmod{n} \\m^{ed} &= m^{1+k \cdot \varphi(n)} = \\&= m^1 \cdot m^{k \cdot \varphi(n)} = \\&= m \cdot (m^{\varphi(n)})^k\end{aligned}$$

Podle Eulerovy věty dostaneme

$$m \cdot (m^{\varphi(n)})^k =$$

Proč to funguje?

$$\begin{aligned}c &= m^{ed} \equiv m \pmod{n} \\m^{ed} &= m^{1+k \cdot \varphi(n)} = \\&= m^1 \cdot m^{k \cdot \varphi(n)} = \\&= m \cdot (m^{\varphi(n)})^k\end{aligned}$$

Podle Eulerovy věty dostaneme

$$\begin{aligned}m \cdot (m^{\varphi(n)})^k &= \\&= m \cdot 1^k =\end{aligned}$$

Proč to funguje?

$$\begin{aligned}c &= m^{ed} \equiv m \pmod{n} \\m^{ed} &= m^{1+k \cdot \varphi(n)} = \\&= m^1 \cdot m^{k \cdot \varphi(n)} = \\&= m \cdot (m^{\varphi(n)})^k\end{aligned}$$

Podle Eulerovy věty dostaneme

$$\begin{aligned}m \cdot (m^{\varphi(n)})^k &= \\&= m \cdot 1^k = \\&= m \cdot 1\end{aligned}$$

Proč to funguje?

$$\begin{aligned}c &= m^{ed} \equiv m \pmod{n} \\m^{ed} &= m^{1+k \cdot \varphi(n)} = \\&= m^1 \cdot m^{k \cdot \varphi(n)} = \\&= m \cdot (m^{\varphi(n)})^k\end{aligned}$$

Podle Eulerovy věty dostaneme

$$\begin{aligned}m \cdot (m^{\varphi(n)})^k &= \\&= m \cdot 1^k = \\&= m \cdot 1 \\&= m\end{aligned}$$

Proč je to bezpečné?

- Eva zná n , e , c
- Aby mohla dešifrovat zprávu, potřebuje $\varphi(n)$...

Proč je to bezpečné?

- Eva zná n , e , c
- Aby mohla dešifrovat zprávu, potřebuje $\varphi(n)$...
 - k tomu by ale potřebovala znát p a q ...

Proč je to bezpečné?

- Eva zná n , e , c
- Aby mohla dešifrovat zprávu, potřebuje $\varphi(n)$...
 - k tomu by ale potřebovala znát p a q ...
 - k tomu by potřebovala rozložit n na p a q
 \Rightarrow hodně hodně hodně **těžké**

Proč je to bezpečné?

- Eva zná n , e , c
- Aby mohla dešifrovat zprávu, potřebuje $\varphi(n)$...
 - k tomu by ale potřebovala znát p a q ...
 - k tomu by potřebovala rozložit n na p a q
 \Rightarrow hodně hodně hodně **těžké**
- $n \sim 2^{2048}$

Proč je to bezpečné?

- Eva zná n , e , c
- Aby mohla dešifrovat zprávu, potřebuje $\varphi(n)$...
 - k tomu by ale potřebovala znát p a q ...
 - k tomu by potřebovala rozložit n na p a q
 \Rightarrow hodně hodně hodně **těžké**
- $n \sim 2^{2048}$
 - $n \sim 10^{600}$

Proč je to bezpečné?

Kolik je 10^{600} ?

Proč je to bezpečné?

Kolik je 10^{600} ?

- 10^{10} ... stáří vesmíru v letech

Proč je to bezpečné?

Kolik je 10^{600} ?

- 10^{10} ... stáří vesmíru v letech
- 10^{43} ... počet všech možných šachových pozic

Proč je to bezpečné?

Kolik je 10^{600} ?

- 10^{10} ... stáří vesmíru v letech
- 10^{43} ... počet všech možných šachových pozic
- 10^{80} ... počet atomů ve vesmíru

Kam dál?

- Problémy diskretního logaritmu a rozkladu jsou **domněnky**¹

¹Žádná z nich není NP-težká, ale NP. Kdyby $P = NP$, problém.

Kam dál?

- Problémy diskretního logaritmu a rozkladu jsou **domněnky**¹
 - Nemusí být pravdivé, nemáme důkaz

¹Žádná z nich není NP-težká, ale NP. Kdyby $P = NP$, problém.

Kam dál?

- Problémy diskrétního logaritmu a rozkladu jsou **domněnky**¹
 - Nemusí být pravdivé, nemáme důkaz
 - Kdybychom našli způsob, jak je spočítat, celá kryptografie by se rozpadla

¹Žádná z nich není NP-težká, ale NP. Kdyby $P = NP$, problém.

Kam dál?

- Problémy diskretního logaritmu a rozkladu jsou **domněnky**¹
 - Nemusí být pravdivé, nemáme důkaz
 - Kdybychom našli způsob, jak je spočítat, celá kryptografie by se rozpadla
- Kvantové algoritmy
 - 1994 Shorův algoritmus řeší problém diskretního logaritmu velmi rychle

¹Žádná z nich není NP-težká, ale NP. Kdyby $P = NP$, problém.

Kam dál?

- Problémy diskretního logaritmu a rozkladu jsou **domněnky**¹
 - Nemusí být pravdivé, nemáme důkaz
 - Kdybychom našli způsob, jak je spočítat, celá kryptografie by se rozpadla
- Kvantové algoritmy
 - 1994 Shorův algoritmus řeší problém diskretního logaritmu velmi rychle
...na kvantovém počítači

¹Žádná z nich není NP-težká, ale NP. Kdyby $P = NP$, problém.

Kam dál?

- Problémy diskrétního logaritmu a rozkladu jsou **domněnky**¹
 - Nemusí být pravdivé, nemáme důkaz
 - Kdybychom našli způsob, jak je spočítat, celá kryptografie by se rozpadla
- Kvantové algoritmy
 - 1994 Shorův algoritmus řeší problém diskrétního logaritmu velmi rychle
 - ...na kvantovém počítači
 - Až budou kvantové počítače dostatečně rychlé, RSA a DHKE se rozpadnou

¹Žádná z nich není NP-težká, ale NP. Kdyby $P = NP$, problém.

Kam dál?

- Nové šifry pro post-kvantovou dobu
 - 2024 NIST, ML-KEM: kryptografie neprolomitelná kvantovými počítači

Kam dál?

- Nové šifry pro post-kvantovou dobu
 - 2024 NIST, ML-KEM: kryptografie neprolomitelná kvantovými počítači
 - ...alespoň to si myslíme

Kam dál?

- Nové šifry pro post-kvantovou dobu
 - 2024 NIST, ML-KEM: kryptografie neprolomitelná kvantovými počítači
 - ...alespoň to si myslíme
- Kde se to, co jsem vám právě ukázal, reálně používá?

Kam dál?

- Nové šifry pro post-kvantovou dobu
 - 2024 NIST, ML-KEM: kryptografie neprolomitelná kvantovými počítači
 - ...alespoň to si myslíme
- Kde se to, co jsem vám právě ukázal, reálně používá?
 - HTTPS (zámeček)
 - WhatsApp, Signal, Messenger
 - Banky, státní instituce

Kam dál?

- Nové šifry pro post-kvantovou dobu
 - 2024 NIST, ML-KEM: kryptografie neprolomitelná kvantovými počítači
 - ...alespoň to si myslíme
- Kde se to, co jsem vám právě ukázal, reálně používá?
 - HTTPS (zámeček)
 - WhatsApp, Signal, Messenger
 - Banky, státní instituce

Všude

Díky za pozornost!