Aplikace algebry: šifrovací systém RSA

Název RSA je tvořen iniciálami autorů (Rivest, Shamir, Adleman).

Aplikace algebry: šifrovací systém RSA

Název RSA je tvořen iniciálami autorů (Rivest, Shamir, Adleman).

Motivace šifrování: posíláme zprávu kanálem, který může být odposloucháván; přitom nechceme, aby naší zprávu uměl přečíst někdo, komu není určena.

Aplikace algebry: šifrovací systém RSA

Název RSA je tvořen iniciálami autorů (Rivest, Shamir, Adleman).

Motivace šifrování: posíláme zprávu kanálem, který může být odposloucháván; přitom nechceme, aby naší zprávu uměl přečíst někdo, komu není určena.

Funkčnost celého systému je založena na tom, že je poměrně snadné vygenerovat dvě velká prvočísla $p \neq q$ a vynásobením najít jejich součin $n = p \cdot q$.

Aplikace algebry: šifrovací systém RSA

Název RSA je tvořen iniciálami autorů (Rivest, Shamir, Adleman).

Motivace šifrování: posíláme zprávu kanálem, který může být odposloucháván; přitom nechceme, aby naší zprávu uměl přečíst někdo, komu není určena.

Funkčnost celého systému je založena na tom, že je poměrně snadné vygenerovat dvě velká prvočísla $p \neq q$ a vynásobením najít jejich součin $n = p \cdot q$.

Víme, že číslo n určuje obě prvočísla p, q jednoznačně.

Aplikace algebry: šifrovací systém RSA

Název RSA je tvořen iniciálami autorů (Rivest, Shamir, Adleman).

Motivace šifrování: posíláme zprávu kanálem, který může být odposloucháván; přitom nechceme, aby naší zprávu uměl přečíst někdo, komu není určena.

Funkčnost celého systému je založena na tom, že je poměrně snadné vygenerovat dvě velká prvočísla $p \neq q$ a vynásobením najít jejich součin $n = p \cdot q$.

Víme, že číslo n určuje obě prvočísla p, q jednoznačně. Pokud jsou však prvočísla p, q obrovská a je splněno několik dalších podmínek, pak není znám žádný algoritmus, kterým bychom je mohli současnou výpočetní technikou v rozumném čase spočítat (výpočet trvající staletí nemá smysl ani začínat).

Aplikace algebry: šifrovací systém RSA

Název RSA je tvořen iniciálami autorů (Rivest, Shamir, Adleman).

Motivace šifrování: posíláme zprávu kanálem, který může být odposloucháván; přitom nechceme, aby naší zprávu uměl přečíst někdo, komu není určena.

Funkčnost celého systému je založena na tom, že je poměrně snadné vygenerovat dvě velká prvočísla $p \neq q$ a vynásobením najít jejich součin $n = p \cdot q$.

Víme, že číslo n určuje obě prvočísla p, q jednoznačně. Pokud jsou však prvočísla p, q obrovská a je splněno několik dalších podmínek, pak není znám žádný algoritmus, kterým bychom je mohli současnou výpočetní technikou v rozumném čase spočítat (výpočet trvající staletí nemá smysl ani začínat).

Tento systém se používá k zabezpečené komunikaci na internetu (například pro internetové bankovnictví).

Aplikace algebry: šifrovací systém RSA

Název RSA je tvořen iniciálami autorů (Rivest, Shamir, Adleman).

Motivace šifrování: posíláme zprávu kanálem, který může být odposloucháván; přitom nechceme, aby naší zprávu uměl přečíst někdo, komu není určena.

Funkčnost celého systému je založena na tom, že je poměrně snadné vygenerovat dvě velká prvočísla $p \neq q$ a vynásobením najít jejich součin $n = p \cdot q$.

Víme, že číslo n určuje obě prvočísla p, q jednoznačně. Pokud jsou však prvočísla p, q obrovská a je splněno několik dalších podmínek, pak není znám žádný algoritmus, kterým bychom je mohli současnou výpočetní technikou v rozumném čase spočítat (výpočet trvající staletí nemá smysl ani začínat).

Tento systém se používá k zabezpečené komunikaci na internetu (například pro internetové bankovnictví). Volba prvočísel, šifrování i dešifrování probíhá zcela automaticky v reálném čase, takže uživatelé si ani neuvědomí, že k šifrování a dešifrování došlo.

Generování tajného a veřejného klíče

Řekněme, že Alice chce poslat zprávu Bobovi.

Generování tajného a veřejného klíče

Řekněme, že Alice chce poslat zprávu Bobovi. Proto si Bob (budoucí příjemce zprávy) vygeneruje svůj tajný a veřejný klíč.

Generování tajného a veřejného klíče

Řekněme, že Alice chce poslat zprávu Bobovi. Proto si Bob (budoucí příjemce zprávy) vygeneruje svůj tajný a veřejný klíč.

Bob si tajně zvolí dvě velká prvočísla p, q (tak, aby měla asi tak 150 dekadických cifer a absolutní hodnota $|p - q|$ jejich rozdílu také alespoň 100 dekadických cifer) a vynásobením najde jejich součin $n = p \cdot q$.

Generování tajného a veřejného klíče

Řekněme, že Alice chce poslat zprávu Bobovi. Proto si Bob (budoucí příjemce zprávy) vygeneruje svůj tajný a veřejný klíč.

Bob si tajně zvolí dvě velká prvočísla p, q (tak, aby měla asi tak 150 dekadických cifer a absolutní hodnota $|p - q|$ jejich rozdílu také alespoň 100 dekadických cifer) a vynásobením najde jejich součin $n = p \cdot q$.

Pak spočítá nejmenší společný násobek k čísel $p - 1$ a $q - 1$ (k tomu využije znalost svých tajných prvočísel p, q) a zvolí přirozené číslo $e > 1$ nesoudělné s k.

Generování tajného a veřejného klíče

Řekněme, že Alice chce poslat zprávu Bobovi. Proto si Bob (budoucí příjemce zprávy) vygeneruje svůj tajný a veřejný klíč.

Bob si tajně zvolí dvě velká prvočísla p, q (tak, aby měla asi tak 150 dekadických cifer a absolutní hodnota $|p - q|$ jejich rozdílu také alespoň 100 dekadických cifer) a vynásobením najde jejich součin $n = p \cdot q$.

Pak spočítá nejmenší společný násobek k čísel $p - 1$ a $q - 1$ (k tomu využije znalost svých tajných prvočísel p, q) a zvolí přirozené číslo $e > 1$ nesoudělné s k.

Pak v grupě $(\mathbb{Z}_k^\times, \cdot)$ najde inverzní prvek $[e]_k^{-1}$ k prvku $[e]_k$ a označí d nejmenší kladný reprezentant třídy $[e]_k^{-1}$.

Generování tajného a veřejného klíče

Řekněme, že Alice chce poslat zprávu Bobovi. Proto si Bob (budoucí příjemce zprávy) vygeneruje svůj tajný a veřejný klíč.

Bob si tajně zvolí dvě velká prvočísla p, q (tak, aby měla asi tak 150 dekadických cifer a absolutní hodnota $|p - q|$ jejich rozdílu také alespoň 100 dekadických cifer) a vynásobením najde jejich součin $n = p \cdot q$.

Pak spočítá nejmenší společný násobek k čísel $p - 1$ a $q - 1$ (k tomu využije znalost svých tajných prvočísel p, q) a zvolí přirozené číslo $e > 1$ nesoudělné s k.

Pak v grupě $(\mathbb{Z}_k^\times, \cdot)$ najde inverzní prvek $[e]_k^{-1}$ k prvku $[e]_k$ a označí d nejmenší kladný reprezentant třídy $[e]_k^{-1}$. Platí tedy $k \mid (ed - 1)$.

Generování tajného a veřejného klíče

Řekněme, že Alice chce poslat zprávu Bobovi. Proto si Bob (budoucí příjemce zprávy) vygeneruje svůj tajný a veřejný klíč.

Bob si tajně zvolí dvě velká prvočísla p, q (tak, aby měla asi tak 150 dekadických cifer a absolutní hodnota $|p - q|$ jejich rozdílu také alespoň 100 dekadických cifer) a vynásobením najde jejich součin $n = p \cdot q$.

Pak spočítá nejmenší společný násobek k čísel $p - 1$ a $q - 1$ (k tomu využije znalost svých tajných prvočísel p, q) a zvolí přirozené číslo $e > 1$ nesoudělné s k.

Pak v grupě $(\mathbb{Z}_k^\times, \cdot)$ najde inverzní prvek $[e]_k^{-1}$ k prvku $[e]_k$ a označí d nejmenší kladný reprezentant třídy $[e]_k^{-1}$. Platí tedy $k \mid (ed - 1)$. (Víme, jak spočítat zbytkovou třídu $[e]_k^{-1}$. Stačí najít koeficienty Bezoutovy rovnosti pro $(e, k) = 1$.)

Generování tajného a veřejného klíče

Řekněme, že Alice chce poslat zprávu Bobovi. Proto si Bob (budoucí příjemce zprávy) vygeneruje svůj tajný a veřejný klíč.

Bob si tajně zvolí dvě velká prvočísla p, q (tak, aby měla asi tak 150 dekadických cifer a absolutní hodnota $|p - q|$ jejich rozdílu také alespoň 100 dekadických cifer) a vynásobením najde jejich součin $n = p \cdot q$.

Pak spočítá nejmenší společný násobek k čísel $p - 1$ a $q - 1$ (k tomu využije znalost svých tajných prvočísel p, q) a zvolí přirozené číslo $e > 1$ nesoudělné s k.

Pak v grupě $(\mathbb{Z}_k^\times, \cdot)$ najde inverzní prvek $[e]_k^{-1}$ k prvku $[e]_k$ a označí d nejmenší kladný reprezentant třídy $[e]_k^{-1}$. Platí tedy $k \mid (ed - 1)$. (Víme, jak spočítat zbytkovou třídu $[e]_k^{-1}$. Stačí najít koeficienty Bezoutovy rovnosti pro $(e, k) = 1$.)

Nyní může komukoli sdělit svůj **veřejný klíč** n, e.

Generování tajného a veřejného klíče

Řekněme, že Alice chce poslat zprávu Bobovi. Proto si Bob (budoucí příjemce zprávy) vygeneruje svůj tajný a veřejný klíč.

Bob si tajně zvolí dvě velká prvočísla p, q (tak, aby měla asi tak 150 dekadických cifer a absolutní hodnota $|p - q|$ jejich rozdílu také alespoň 100 dekadických cifer) a vynásobením najde jejich součin $n = p \cdot q$.

Pak spočítá nejmenší společný násobek k čísel $p - 1$ a $q - 1$ (k tomu využije znalost svých tajných prvočísel p, q) a zvolí přirozené číslo $e > 1$ nesoudělné s k.

Pak v grupě $(\mathbb{Z}_k^\times, \cdot)$ najde inverzní prvek $[e]_k^{-1}$ k prvku $[e]_k$ a označí d nejmenší kladný reprezentant třídy $[e]_k^{-1}$. Platí tedy $k \mid (ed - 1)$. (Víme, jak spočítat zbytkovou třídu $[e]_k^{-1}$. Stačí najít koeficienty Bezoutovy rovnosti pro $(e, k) = 1$.)

Nyní může komukoli sdělit svůj **veřejný klíč** n, e.

Jeho **tajný klíč**, který neprozradí ani Alici, je znalost čísla d (a prvočísel p, q, pomocí kterých je možné číslo d vypočítat).

Zašifrování a dešifrování zprávy

Alice chce Bobovi odeslat zprávu.

Zašifrování a dešifrování zprávy

Alice chce Bobovi odeslat zprávu. Zjistí si Bobův veřejný klíč n, e (musí si ovšem být jista, že tento veřejný klíč je opravdu Bobův a ne někoho jiného, kdo se jen za Boba vydává).

Zašifrování a dešifrování zprávy

Alice chce Bobovi odeslat zprávu. Zjistí si Bobův veřejný klíč n, e (musí si ovšem být jista, že tento veřejný klíč je opravdu Bobův a ne někoho jiného, kdo se jen za Boba vydává).

Není nijak omezující předpokládat, že touto zprávou je celé číslo m splňující $1 < m < n$.

Zašifrování a dešifrování zprávy

Alice chce Bobovi odeslat zprávu. Zjistí si Bobův veřejný klíč n, e (musí si ovšem být jista, že tento veřejný klíč je opravdu Bobův a ne někoho jiného, kdo se jen za Boba vydává).

Není nijak omezující předpokládat, že touto zprávou je celé číslo m splňující $1 < m < n$.

Alice najde zbytek z po dělení čísla m^e číslem n (ukážeme si algoritmus pro tento výpočet, který je rychlý, přestože čísla m, e, n jsou velká) a pošle Bobovi jako svou zprávu číslo z.

Zašifrování a dešifrování zprávy

Alice chce Bobovi odeslat zprávu. Zjistí si Bobův veřejný klíč n, e (musí si ovšem být jista, že tento veřejný klíč je opravdu Bobův a ne někoho jiného, kdo se jen za Boba vydává).

Není nijak omezující předpokládat, že touto zprávou je celé číslo m splňující $1 < m < n$.

Alice najde zbytek z po dělení čísla m^e číslem n (ukážeme si algoritmus pro tento výpočet, který je rychlý, přestože čísla m, e, n jsou velká) a pošle Bobovi jako svou zprávu číslo z.

Bob obdrží od Alice číslo z, využije svůj tajný klíč d a najde zbytek w po dělení čísla z^d číslem n (zmíněným rychlým algoritmem).

Zašifrování a dešifrování zprávy

Alice chce Bobovi odeslat zprávu. Zjistí si Bobův veřejný klíč n, e (musí si ovšem být jista, že tento veřejný klíč je opravdu Bobův a ne někoho jiného, kdo se jen za Boba vydává).

Není nijak omezující předpokládat, že touto zprávou je celé číslo m splňující $1 < m < n$.

Alice najde zbytek z po dělení čísla m^e číslem n (ukážeme si algoritmus pro tento výpočet, který je rychlý, přestože čísla m, e, n jsou velká) a pošle Bobovi jako svou zprávu číslo z.

Bob obdrží od Alice číslo z, využije svůj tajný klíč d a najde zbytek w po dělení čísla z^d číslem n (zmíněným rychlým algoritmem).

Bob tím získal zprávu, kterou mu Alice chtěla poslat, neboť platí $m = w$ (to si dokážeme).

Zašifrování a dešifrování zprávy

Alice chce Bobovi odeslat zprávu. Zjistí si Bobův veřejný klíč n, e (musí si ovšem být jista, že tento veřejný klíč je opravdu Bobův a ne někoho jiného, kdo se jen za Boba vydává).

Není nijak omezující předpokládat, že touto zprávou je celé číslo m splňující $1 < m < n$.

Alice najde zbytek z po dělení čísla m^e číslem n (ukážeme si algoritmus pro tento výpočet, který je rychlý, přestože čísla m, e, n jsou velká) a pošle Bobovi jako svou zprávu číslo z.

Bob obdrží od Alice číslo z, využije svůj tajný klíč d a najde zbytek w po dělení čísla z^d číslem n (zmíněným rychlým algoritmem).

Bob tím získal zprávu, kterou mu Alice chtěla poslat, neboť platí $m = w$ (to si dokážeme).

Bez dalších detailů zmiňme, že tento systém je možné vybavit i podepisováním zpráv (aby si byl Bob jist, že dostal nepoškozenou a nepodvrženou zprávu skutečně od Alice).

Zašifrování a dešifrování zprávy

Alice chce Bobovi odeslat zprávu. Zjistí si Bobův veřejný klíč n, e (musí si ovšem být jista, že tento veřejný klíč je opravdu Bobův a ne někoho jiného, kdo se jen za Boba vydává).

Není nijak omezující předpokládat, že touto zprávou je celé číslo m splňující $1 < m < n$.

Alice najde zbytek z po dělení čísla m^e číslem n (ukážeme si algoritmus pro tento výpočet, který je rychlý, přestože čísla m, e, n jsou velká) a pošle Bobovi jako svou zprávu číslo z.

Bob obdrží od Alice číslo z, využije svůj tajný klíč d a najde zbytek w po dělení čísla z^d číslem n (zmíněným rychlým algoritmem).

Bob tím získal zprávu, kterou mu Alice chtěla poslat, neboť platí $m = w$ (to si dokážeme).

Bez dalších detailů zmiňme, že tento systém je možné vybavit i podepisováním zpráv (aby si byl Bob jist, že dostal nepoškozenou a nepodvrženou zprávu skutečně od Alice). Je při tom využit veřejný a tajný klíč, který si stejným způsobem zvolí Alice.

Důkaz správného dešifrování zprávy

$p \neq q$ velká prvočísla, $n = p \cdot q$, $k = [p-1, q-1] = \frac{(p-1)(q-1)}{(p-1,q-1)}$,
$e > 1$, $d > 1$, $k \mid (ed-1)$, $1 < m < n$, $[z]_n = [m^e]_n$, $[w]_n = [z^d]_n$,
$0 \leq w < n$.

Důkaz správného dešifrování zprávy

$p \neq q$ velká prvočísla, $n = p \cdot q$, $k = [p-1, q-1] = \frac{(p-1)(q-1)}{(p-1,q-1)}$, $e > 1$, $d > 1$, $k \mid (ed-1)$, $1 < m < n$, $[z]_n = [m^e]_n$, $[w]_n = [z^d]_n$, $0 \leq w < n$.

Platí $[z]_n = [m^e]_n$, a tedy $[w]_n = [z^d]_n = [z]_n^d = [m^e]_n^d = [m^{ed}]_n$.

Důkaz správného dešifrování zprávy

$p \neq q$ velká prvočísla, $n = p \cdot q$, $k = [p-1, q-1] = \frac{(p-1)(q-1)}{(p-1,q-1)}$,
$e > 1$, $d > 1$, $k \mid (ed-1)$, $1 < m < n$, $[z]_n = [m^e]_n$, $[w]_n = [z^d]_n$,
$0 \leq w < n$.

Platí $[z]_n = [m^e]_n$, a tedy $[w]_n = [z^d]_n = [z]_n^d = [m^e]_n^d = [m^{ed}]_n$.
Dokážeme $[w]_n = [m]_n$, tj. $[m^{ed}]_n = [m]_n$, tedy že $n \mid (m^{ed} - m)$.

Důkaz správného dešifrování zprávy

$p \neq q$ velká prvočísla, $n = p \cdot q$, $k = [p-1, q-1] = \frac{(p-1)(q-1)}{(p-1,q-1)}$,
$e > 1$, $d > 1$, $k \mid (ed-1)$, $1 < m < n$, $[z]_n = [m^e]_n$, $[w]_n = [z^d]_n$,
$0 \leq w < n$.

Platí $[z]_n = [m^e]_n$, a tedy $[w]_n = [z^d]_n = [z]_n^d = [m^e]_n^d = [m^{ed}]_n$.
Dokážeme $[w]_n = [m]_n$, tj. $[m^{ed}]_n = [m]_n$, tedy že $n \mid (m^{ed} - m)$.
Postačí dokázat, že $p \mid (m^{ed} - m)$ a současně $q \mid (m^{ed} - m)$.

Důkaz správného dešifrování zprávy

$p \neq q$ velká prvočísla, $n = p \cdot q$, $k = [p-1, q-1] = \frac{(p-1)(q-1)}{(p-1,q-1)}$, $e > 1$, $d > 1$, $k \mid (ed-1)$, $1 < m < n$, $[z]_n = [m^e]_n$, $[w]_n = [z^d]_n$, $0 \leq w < n$.

Platí $[z]_n = [m^e]_n$, a tedy $[w]_n = [z^d]_n = [z]_n^d = [m^e]_n^d = [m^{ed}]_n$.
Dokážeme $[w]_n = [m]_n$, tj. $[m^{ed}]_n = [m]_n$, tedy že $n \mid (m^{ed} - m)$.
Postačí dokázat, že $p \mid (m^{ed} - m)$ a současně $q \mid (m^{ed} - m)$.
Ukažme, jak dokázat první dělitelnost (druhá se dokáže analogicky, neboť prvočísla p a q v úloze vystupují symetricky).

Důkaz správného dešifrování zprávy

$p \neq q$ velká prvočísla, $n = p \cdot q$, $k = [p-1, q-1] = \frac{(p-1)(q-1)}{(p-1,q-1)}$, $e > 1$, $d > 1$, $k \mid (ed-1)$, $1 < m < n$, $[z]_n = [m^e]_n$, $[w]_n = [z^d]_n$, $0 \leq w < n$.

Platí $[z]_n = [m^e]_n$, a tedy $[w]_n = [z^d]_n = [z]_n^d = [m^e]_n^d = [m^{ed}]_n$.
Dokážeme $[w]_n = [m]_n$, tj. $[m^{ed}]_n = [m]_n$, tedy že $n \mid (m^{ed} - m)$.
Postačí dokázat, že $p \mid (m^{ed} - m)$ a současně $q \mid (m^{ed} - m)$.
Ukažme, jak dokázat první dělitelnost (druhá se dokáže analogicky, neboť prvočísla p a q v úloze vystupují symetricky).
Protože $p - 1 \mid k$, $k \mid (ed-1)$, platí $p - 1 \mid (ed-1)$.

Důkaz správného dešifrování zprávy

$p \neq q$ velká prvočísla, $n = p \cdot q$, $k = [p-1, q-1] = \frac{(p-1)(q-1)}{(p-1,q-1)}$,
$e > 1$, $d > 1$, $k \mid (ed-1)$, $1 < m < n$, $[z]_n = [m^e]_n$, $[w]_n = [z^d]_n$,
$0 \leq w < n$.

Platí $[z]_n = [m^e]_n$, a tedy $[w]_n = [z^d]_n = [z]_n^d = [m^e]_n^d = [m^{ed}]_n$.
Dokážeme $[w]_n = [m]_n$, tj. $[m^{ed}]_n = [m]_n$, tedy že $n \mid (m^{ed} - m)$.
Postačí dokázat, že $p \mid (m^{ed} - m)$ a současně $q \mid (m^{ed} - m)$.
Ukažme, jak dokázat první dělitelnost (druhá se dokáže analogicky, neboť prvočísla p a q v úloze vystupují symetricky).
Protože $p - 1 \mid k$, $k \mid (ed-1)$, platí $p - 1 \mid (ed-1)$.
Rozlišíme dva případy:
Jestliže $p \mid m$, pak $p \mid m \cdot (m^{ed-1} - 1) = (m^{ed} - m)$.

Důkaz správného dešifrování zprávy

$p \neq q$ velká prvočísla, $n = p \cdot q$, $k = [p-1, q-1] = \frac{(p-1)(q-1)}{(p-1,q-1)}$,
$e > 1$, $d > 1$, $k \mid (ed-1)$, $1 < m < n$, $[z]_n = [m^e]_n$, $[w]_n = [z^d]_n$,
$0 \leq w < n$.

Platí $[z]_n = [m^e]_n$, a tedy $[w]_n = [z^d]_n = [z]_n^d = [m^e]_n^d = [m^{ed}]_n$.
Dokážeme $[w]_n = [m]_n$, tj. $[m^{ed}]_n = [m]_n$, tedy že $n \mid (m^{ed} - m)$.
Postačí dokázat, že $p \mid (m^{ed} - m)$ a současně $q \mid (m^{ed} - m)$.
Ukažme, jak dokázat první dělitelnost (druhá se dokáže analogicky, neboť prvočísla p a q v úloze vystupují symetricky).
Protože $p - 1 \mid k$, $k \mid (ed-1)$, platí $p - 1 \mid (ed-1)$.
Rozlišíme dva případy:
Jestliže $p \mid m$, pak $p \mid m \cdot (m^{ed-1} - 1) = (m^{ed} - m)$.
Jestliže naopak $p \nmid m$, pak $(p, m) = 1$, neboť p je prvočíslo.

Důkaz správného dešifrování zprávy

$p \neq q$ velká prvočísla, $n = p \cdot q$, $k = [p-1, q-1] = \frac{(p-1)(q-1)}{(p-1,q-1)}$,
$e > 1$, $d > 1$, $k \mid (ed-1)$, $1 < m < n$, $[z]_n = [m^e]_n$, $[w]_n = [z^d]_n$,
$0 \leq w < n$.

Platí $[z]_n = [m^e]_n$, a tedy $[w]_n = [z^d]_n = [z]_n^d = [m^e]_n^d = [m^{ed}]_n$.
Dokážeme $[w]_n = [m]_n$, tj. $[m^{ed}]_n = [m]_n$, tedy že $n \mid (m^{ed} - m)$.
Postačí dokázat, že $p \mid (m^{ed} - m)$ a současně $q \mid (m^{ed} - m)$.
Ukažme, jak dokázat první dělitelnost (druhá se dokáže analogicky, neboť prvočísla p a q v úloze vystupují symetricky).
Protože $p - 1 \mid k$, $k \mid (ed-1)$, platí $p - 1 \mid (ed-1)$.
Rozlišíme dva případy:
Jestliže $p \mid m$, pak $p \mid m \cdot (m^{ed-1} - 1) = (m^{ed} - m)$.
Jestliže naopak $p \nmid m$, pak $(p, m) = 1$, neboť p je prvočíslo.
Eulerova věta dává $m^{p-1} \equiv 1 \pmod{p}$, tj. $[m]_p^{p-1} = [1]_p$.

Důkaz správného dešifrování zprávy

$p \neq q$ velká prvočísla, $n = p \cdot q$, $k = [p-1, q-1] = \frac{(p-1)(q-1)}{(p-1,q-1)}$,
$e > 1$, $d > 1$, $k \mid (ed-1)$, $1 < m < n$, $[z]_n = [m^e]_n$, $[w]_n = [z^d]_n$,
$0 \leq w < n$.

Platí $[z]_n = [m^e]_n$, a tedy $[w]_n = [z^d]_n = [z]_n^d = [m^e]_n^d = [m^{ed}]_n$.
Dokážeme $[w]_n = [m]_n$, tj. $[m^{ed}]_n = [m]_n$, tedy že $n \mid (m^{ed} - m)$.
Postačí dokázat, že $p \mid (m^{ed} - m)$ a současně $q \mid (m^{ed} - m)$.
Ukažme, jak dokázat první dělitelnost (druhá se dokáže analogicky, neboť prvočísla p a q v úloze vystupují symetricky).
Protože $p - 1 \mid k$, $k \mid (ed-1)$, platí $p - 1 \mid (ed-1)$.
Rozlišíme dva případy:
Jestliže $p \mid m$, pak $p \mid m \cdot (m^{ed-1} - 1) = (m^{ed} - m)$.
Jestliže naopak $p \nmid m$, pak $(p, m) = 1$, neboť p je prvočíslo.
Eulerova věta dává $m^{p-1} \equiv 1 \pmod{p}$, tj. $[m]_p^{p-1} = [1]_p$.
Umocněním na přirozené číslo $\frac{ed-1}{p-1}$ dostaneme $[m]_p^{ed-1} = [1]_p$, a tedy $p \mid (m^{ed-1} - 1)$.

Důkaz správného dešifrování zprávy

$p \neq q$ velká prvočísla, $n = p \cdot q$, $k = [p-1, q-1] = \frac{(p-1)(q-1)}{(p-1,q-1)}$,
$e > 1$, $d > 1$, $k \mid (ed-1)$, $1 < m < n$, $[z]_n = [m^e]_n$, $[w]_n = [z^d]_n$,
$0 \leq w < n$.

Platí $[z]_n = [m^e]_n$, a tedy $[w]_n = [z^d]_n = [z]_n^d = [m^e]_n^d = [m^{ed}]_n$.
Dokážeme $[w]_n = [m]_n$, tj. $[m^{ed}]_n = [m]_n$, tedy že $n \mid (m^{ed} - m)$.
Postačí dokázat, že $p \mid (m^{ed} - m)$ a současně $q \mid (m^{ed} - m)$.
Ukažme, jak dokázat první dělitelnost (druhá se dokáže analogicky, neboť prvočísla p a q v úloze vystupují symetricky).
Protože $p - 1 \mid k$, $k \mid (ed-1)$, platí $p - 1 \mid (ed-1)$.
Rozlišíme dva případy:
Jestliže $p \mid m$, pak $p \mid m \cdot (m^{ed-1} - 1) = (m^{ed} - m)$.
Jestliže naopak $p \nmid m$, pak $(p, m) = 1$, neboť p je prvočíslo.
Eulerova věta dává $m^{p-1} \equiv 1 \pmod{p}$, tj. $[m]_p^{p-1} = [1]_p$.
Umocněním na přirozené číslo $\frac{ed-1}{p-1}$ dostaneme $[m]_p^{ed-1} = [1]_p$, a tedy $p \mid (m^{ed-1} - 1)$. Odtud opět $p \mid m \cdot (m^{ed-1} - 1) = (m^{ed} - m)$.

Důkaz správného dešifrování zprávy

$p \neq q$ velká prvočísla, $n = p \cdot q$, $k = [p-1, q-1] = \frac{(p-1)(q-1)}{(p-1,q-1)}$, $e > 1$, $d > 1$, $k \mid (ed-1)$, $1 < m < n$, $[z]_n = [m^e]_n$, $[w]_n = [z^d]_n$, $0 \leq w < n$.

Platí $[z]_n = [m^e]_n$, a tedy $[w]_n = [z^d]_n = [z]_n^d = [m^e]_n^d = [m^{ed}]_n$.
Dokážeme $[w]_n = [m]_n$, tj. $[m^{ed}]_n = [m]_n$, tedy že $n \mid (m^{ed} - m)$.
Postačí dokázat, že $p \mid (m^{ed} - m)$ a současně $q \mid (m^{ed} - m)$.
Ukažme, jak dokázat první dělitelnost (druhá se dokáže analogicky, neboť prvočísla p a q v úloze vystupují symetricky).
Protože $p - 1 \mid k$, $k \mid (ed-1)$, platí $p - 1 \mid (ed-1)$.
Rozlišíme dva případy:
Jestliže $p \mid m$, pak $p \mid m \cdot (m^{ed-1} - 1) = (m^{ed} - m)$.
Jestliže naopak $p \nmid m$, pak $(p, m) = 1$, neboť p je prvočíslo.
Eulerova věta dává $m^{p-1} \equiv 1 \pmod{p}$, tj. $[m]_p^{p-1} = [1]_p$.
Umocněním na přirozené číslo $\frac{ed-1}{p-1}$ dostaneme $[m]_p^{ed-1} = [1]_p$, a tedy $p \mid (m^{ed-1} - 1)$. Odtud opět $p \mid m \cdot (m^{ed-1} - 1) = (m^{ed} - m)$.
Dostali jsme $n \mid (m - w)$, což spolu s $1 < m < n$, $0 \leq w < n$ dává $m = w$.

Rychlé umocňování

Při šifrování své zprávy potřebuje Alice spočítat zbytek z po dělení čísla m^e číslem n.

Rychlé umocňování

Při šifrování své zprávy potřebuje Alice spočítat zbytek z po dělení čísla m^e číslem n. Nejprve vyjádří exponent e ve dvojkové soustavě:

$$e = 2^r a_r + 2^{r-1} a_{r-1} + \cdots + 4a_2 + 2a_1 + a_0,$$

kde $a_0, a_1, \ldots, a_r \in \{0, 1\}$.

Rychlé umocňování

Při šifrování své zprávy potřebuje Alice spočítat zbytek z po dělení čísla m^e číslem n. Nejprve vyjádří exponent e ve dvojkové soustavě:

$$e = 2^r a_r + 2^{r-1} a_{r-1} + \cdots + 4a_2 + 2a_1 + a_0,$$

kde $a_0, a_1, \ldots, a_r \in \{0, 1\}$.

Pak postupně násobením umocňuje na druhou a výsledek dělí se zbytkem číslem n, aby dostala čísla $t_1 \equiv m^2 \pmod{n}$, $0 \leq t_1 < n$,

Rychlé umocňování

Při šifrování své zprávy potřebuje Alice spočítat zbytek z po dělení čísla m^e číslem n. Nejprve vyjádří exponent e ve dvojkové soustavě:

$$e = 2^r a_r + 2^{r-1} a_{r-1} + \cdots + 4a_2 + 2a_1 + a_0,$$

kde $a_0, a_1, \ldots, a_r \in \{0, 1\}$.

Pak postupně násobením umocňuje na druhou a výsledek dělí se zbytkem číslem n, aby dostala čísla $t_1 \equiv m^2 \pmod{n}$, $0 \leq t_1 < n$, $t_2 \equiv t_1^2 \pmod{n}$, $0 \leq t_2 < n$,

Rychlé umocňování

Při šifrování své zprávy potřebuje Alice spočítat zbytek z po dělení čísla m^e číslem n. Nejprve vyjádří exponent e ve dvojkové soustavě:

$$e = 2^r a_r + 2^{r-1} a_{r-1} + \cdots + 4a_2 + 2a_1 + a_0,$$

kde $a_0, a_1, \ldots, a_r \in \{0, 1\}$.

Pak postupně násobením umocňuje na druhou a výsledek dělí se zbytkem číslem n, aby dostala čísla $t_1 \equiv m^2 \pmod{n}$, $0 \leq t_1 < n$, $t_2 \equiv t_1^2 \pmod{n}$, $0 \leq t_2 < n$, $t_3 \equiv t_2^2 \pmod{n}$, $0 \leq t_3 < n$,

Rychlé umocňování

Při šifrování své zprávy potřebuje Alice spočítat zbytek z po dělení čísla m^e číslem n. Nejprve vyjádří exponent e ve dvojkové soustavě:

$$e = 2^r a_r + 2^{r-1} a_{r-1} + \cdots + 4a_2 + 2a_1 + a_0,$$

kde $a_0, a_1, \ldots, a_r \in \{0, 1\}$.

Pak postupně násobením umocňuje na druhou a výsledek dělí se zbytkem číslem n, aby dostala čísla $t_1 \equiv m^2 \pmod{n}$, $0 \leq t_1 < n$, $t_2 \equiv t_1^2 \pmod{n}$, $0 \leq t_2 < n$, $t_3 \equiv t_2^2 \pmod{n}$, $0 \leq t_3 < n$, $\ldots$, $t_r \equiv t_{r-1}^2 \pmod{n}$, $0 \leq t_r < n$.

Rychlé umocňování

Při šifrování své zprávy potřebuje Alice spočítat zbytek z po dělení čísla m^e číslem n. Nejprve vyjádří exponent e ve dvojkové soustavě:

$$e = 2^r a_r + 2^{r-1} a_{r-1} + \cdots + 4a_2 + 2a_1 + a_0,$$

kde $a_0, a_1, \ldots, a_r \in \{0, 1\}$.

Pak postupně násobením umocňuje na druhou a výsledek dělí se zbytkem číslem n, aby dostala čísla $t_1 \equiv m^2 \pmod{n}$, $0 \leq t_1 < n$, $t_2 \equiv t_1^2 \pmod{n}$, $0 \leq t_2 < n$, $t_3 \equiv t_2^2 \pmod{n}$, $0 \leq t_3 < n$, $\ldots$, $t_r \equiv t_{r-1}^2 \pmod{n}$, $0 \leq t_r < n$. Označme $t_0 = m$.

Rychlé umocňování

Při šifrování své zprávy potřebuje Alice spočítat zbytek z po dělení čísla m^e číslem n. Nejprve vyjádří exponent e ve dvojkové soustavě:

$$e = 2^r a_r + 2^{r-1} a_{r-1} + \cdots + 4a_2 + 2a_1 + a_0,$$

kde $a_0, a_1, \ldots, a_r \in \{0, 1\}$.

Pak postupně násobením umocňuje na druhou a výsledek dělí se zbytkem číslem n, aby dostala čísla $t_1 \equiv m^2 \pmod{n}$, $0 \leq t_1 < n$, $t_2 \equiv t_1^2 \pmod{n}$, $0 \leq t_2 < n$, $t_3 \equiv t_2^2 \pmod{n}$, $0 \leq t_3 < n$, $\ldots$, $t_r \equiv t_{r-1}^2 \pmod{n}$, $0 \leq t_r < n$. Označme $t_0 = m$.

Platí tedy $t_i \equiv m^{2^i} \pmod{n}$ pro každé $i = 0, 1, 2, \ldots, r$.

Rychlé umocňování

Při šifrování své zprávy potřebuje Alice spočítat zbytek z po dělení čísla m^e číslem n. Nejprve vyjádří exponent e ve dvojkové soustavě:

$$e = 2^r a_r + 2^{r-1} a_{r-1} + \cdots + 4a_2 + 2a_1 + a_0,$$

kde $a_0, a_1, \ldots, a_r \in \{0, 1\}$.

Pak postupně násobením umocňuje na druhou a výsledek dělí se zbytkem číslem n, aby dostala čísla $t_1 \equiv m^2 \pmod{n}$, $0 \leq t_1 < n$, $t_2 \equiv t_1^2 \pmod{n}$, $0 \leq t_2 < n$, $t_3 \equiv t_2^2 \pmod{n}$, $0 \leq t_3 < n$, $\ldots$, $t_r \equiv t_{r-1}^2 \pmod{n}$, $0 \leq t_r < n$. Označme $t_0 = m$.

Platí tedy $t_i \equiv m^{2^i} \pmod{n}$ pro každé $i = 0, 1, 2, \ldots, r$.

Pak postupně vynásobí všechna t_i, pro která $a_i = 1$ (přitom po každém násobení nahradí součin jeho zbytkem po dělení číslem n).

Rychlé umocňování

Při šifrování své zprávy potřebuje Alice spočítat zbytek z po dělení čísla m^e číslem n. Nejprve vyjádří exponent e ve dvojkové soustavě:

$$e = 2^r a_r + 2^{r-1} a_{r-1} + \cdots + 4a_2 + 2a_1 + a_0,$$

kde $a_0, a_1, \ldots, a_r \in \{0, 1\}$.

Pak postupně násobením umocňuje na druhou a výsledek dělí se zbytkem číslem n, aby dostala čísla $t_1 \equiv m^2 \pmod{n}$, $0 \leq t_1 < n$, $t_2 \equiv t_1^2 \pmod{n}$, $0 \leq t_2 < n$, $t_3 \equiv t_2^2 \pmod{n}$, $0 \leq t_3 < n$, $\ldots$, $t_r \equiv t_{r-1}^2 \pmod{n}$, $0 \leq t_r < n$. Označme $t_0 = m$.

Platí tedy $t_i \equiv m^{2^i} \pmod{n}$ pro každé $i = 0, 1, 2, \ldots, r$.

Pak postupně vynásobí všechna t_i, pro která $a_i = 1$ (přitom po každém násobení nahradí součin jeho zbytkem po dělení číslem n). Tím dostane $z \equiv \prod_{i=0}^{r} t_i^{a_i} \equiv \prod_{i=0}^{r} m^{2^i a_i} \equiv m^e \pmod{n}$.

Rychlé umocňování

Při šifrování své zprávy potřebuje Alice spočítat zbytek z po dělení čísla m^e číslem n. Nejprve vyjádří exponent e ve dvojkové soustavě:

$$e = 2^r a_r + 2^{r-1} a_{r-1} + \cdots + 4a_2 + 2a_1 + a_0,$$

kde $a_0, a_1, \ldots, a_r \in \{0, 1\}$.

Pak postupně násobením umocňuje na druhou a výsledek dělí se zbytkem číslem n, aby dostala čísla $t_1 \equiv m^2 \pmod{n}$, $0 \leq t_1 < n$, $t_2 \equiv t_1^2 \pmod{n}$, $0 \leq t_2 < n$, $t_3 \equiv t_2^2 \pmod{n}$, $0 \leq t_3 < n$, $\ldots$, $t_r \equiv t_{r-1}^2 \pmod{n}$, $0 \leq t_r < n$. Označme $t_0 = m$.

Platí tedy $t_i \equiv m^{2^i} \pmod{n}$ pro každé $i = 0, 1, 2, \ldots, r$.

Pak postupně vynásobí všechna t_i, pro která $a_i = 1$ (přitom po každém násobení nahradí součin jeho zbytkem po dělení číslem n). Tím dostane $z \equiv \prod_{i=0}^{r} t_i^{a_i} \equiv \prod_{i=0}^{r} m^{2^i a_i} \equiv m^e \pmod{n}$.

Může být výhodnější raději než se zbytky pracovat v průběhu výpočtu s celými čísly z intervalu $(-\frac{n}{2}, \frac{n}{2})$, neboť pak násobíme čísla s menší absolutní hodnotou.

Volba velkých prvočísel

Vysvětleme si, jak bude Bob volit velká prvočísla.

Volba velkých prvočísel

Vysvětleme si, jak bude Bob volit velká prvočísla.

Může náhodně zvolit liché číslo vhodné velikosti a otestovat, zda toto číslo je či není prvočíslo.

Volba velkých prvočísel

Vysvětleme si, jak bude Bob volit velká prvočísla.

Může náhodně zvolit liché číslo vhodné velikosti a otestovat, zda toto číslo je či není prvočíslo. Test, který navrhli M.O. Rabin a G.L. Miller je založen na následující větě:

Věta. Nechť p je liché prvočíslo. Pišme $p - 1 = 2^t \cdot \ell$, kde t je přirozené číslo a ℓ je liché.

Volba velkých prvočísel

Vysvětleme si, jak bude Bob volit velká prvočísla.

Může náhodně zvolit liché číslo vhodné velikosti a otestovat, zda toto číslo je či není prvočíslo. Test, který navrhli M.O. Rabin a G.L. Miller je založen na následující větě:

Věta. *Nechť p je liché prvočíslo. Pišme $p-1 = 2^t \cdot \ell$, kde t je přirozené číslo a ℓ je liché. Pak pro každé celé číslo a nedělitelné p buď platí $a^\ell \equiv 1 \pmod{p}$ nebo existuje $e \in \{0, 1, \ldots, t-1\}$ splňující $a^{2^e \ell} \equiv -1 \pmod{p}$.*

Volba velkých prvočísel

Vysvětleme si, jak bude Bob volit velká prvočísla.

Může náhodně zvolit liché číslo vhodné velikosti a otestovat, zda toto číslo je či není prvočíslo. Test, který navrhli M.O. Rabin a G.L. Miller je založen na následující větě:

Věta. *Nechť p je liché prvočíslo. Pišme $p-1 = 2^t \cdot \ell$, kde t je přirozené číslo a ℓ je liché. Pak pro každé celé číslo a nedělitelné p buď platí $a^\ell \equiv 1 \pmod{p}$ nebo existuje $e \in \{0, 1, \ldots, t-1\}$ splňující $a^{2^e \ell} \equiv -1 \pmod{p}$.*

Důkaz. Z Eulerovy věty užitím vzorce pro rozklad rozdílu druhých mocnin

$$p \mid (a^{p-1} - 1) = (a^\ell - 1) \cdot \prod_{e=0}^{t-1} (a^{2^e \ell} + 1).$$

Volba velkých prvočísel

Vysvětleme si, jak bude Bob volit velká prvočísla.

Může náhodně zvolit liché číslo vhodné velikosti a otestovat, zda toto číslo je či není prvočíslo. Test, který navrhli M.O. Rabin a G.L. Miller je založen na následující větě:

Věta. *Nechť p je liché prvočíslo. Pišme $p-1 = 2^t \cdot \ell$, kde t je přirozené číslo a ℓ je liché. Pak pro každé celé číslo a nedělitelné p buď platí $a^\ell \equiv 1 \pmod{p}$ nebo existuje $e \in \{0, 1, \ldots, t-1\}$ splňující $a^{2^e \ell} \equiv -1 \pmod{p}$.*

Důkaz. Z Eulerovy věty užitím vzorce pro rozklad rozdílu druhých mocnin

$$p \mid (a^{p-1} - 1) = (a^\ell - 1) \cdot \prod_{e=0}^{t-1} (a^{2^e \ell} + 1).$$

Protože je p prvočíslo, musí dělit některého z uvedených činitelů.

Teoretický základ testu Rabina a Millera

Věta. *Nechť $N > 10$ je liché složené číslo. Pišme $N - 1 = 2^t \cdot \ell$, kde t je přirozené číslo a ℓ je liché.*

Teoretický základ testu Rabina a Millera

Věta. *Nechť $N > 10$ je liché složené číslo. Pišme $N - 1 = 2^t \cdot \ell$, kde t je přirozené číslo a ℓ je liché. Pak nejvýše čtvrtina z čísel množiny $\{a \in \mathbb{Z};\ 1 \leq a < N,\ (a, N) = 1\}$ splňuje následující podmínku:*

$$a^{\ell} \equiv 1 \pmod{N}$$

nebo existuje $e \in \{0, 1, \ldots, t-1\}$ splňující

$$a^{2^e \ell} \equiv -1 \pmod{N}.$$

Teoretický základ testu Rabina a Millera

Věta. *Nechť $N > 10$ je liché složené číslo. Pišme $N - 1 = 2^t \cdot \ell$, kde t je přirozené číslo a ℓ je liché. Pak nejvýše čtvrtina z čísel množiny $\{a \in \mathbb{Z};\ 1 \leq a < N,\ (a, N) = 1\}$ splňuje následující podmínku:*

$$a^{\ell} \equiv 1 \pmod{N}$$

nebo existuje $e \in \{0, 1, \ldots, t-1\}$ splňující

$$a^{2^e \ell} \equiv -1 \pmod{N}.$$

Důkaz je zdlouhavý a rozpadá se na probírání několika speciálních případů, a proto si jej nebudeme uvádět, přestože nepoužívá nic, co by nebylo možné v rámci naší přednášky vysvětlit.

Test Rabina a Millera

Pro dané N algoritmus otestuje podmínku předchozí věty pro předem daný počet r náhodně zvolených celých čísel a splňujících $1 < a < N - 1$.

Test Rabina a Millera

Pro dané N algoritmus otestuje podmínku předchozí věty pro předem daný počet r náhodně zvolených celých čísel a splňujících $1 < a < N - 1$. Pokud pro některé takové a není podmínka splněna, algoritmus odpoví, že N je složené.

Test Rabina a Millera

Pro dané N algoritmus otestuje podmínku předchozí věty pro předem daný počet r náhodně zvolených celých čísel a splňujících $1 < a < N - 1$. Pokud pro některé takové a není podmínka splněna, algoritmus odpoví, že N je složené. Pokud je splněna podmínka pro každé takové a, algoritmus odpoví, že N je asi prvočíslo.

Test Rabina a Millera

Pro dané N algoritmus otestuje podmínku předchozí věty pro předem daný počet r náhodně zvolených celých čísel a splňujících $1 < a < N - 1$. Pokud pro některé takové a není podmínka splněna, algoritmus odpoví, že N je složené. Pokud je splněna podmínka pro každé takové a, algoritmus odpoví, že N je asi prvočíslo.

Je nenulová pravděpodobnost, že algoritmus odpoví, že N je asi prvočíslo, přestože ve skutečnosti je N složené.

Test Rabina a Millera

Pro dané N algoritmus otestuje podmínku předchozí věty pro předem daný počet r náhodně zvolených celých čísel a splňujících $1 < a < N - 1$. Pokud pro některé takové a není podmínka splněna, algoritmus odpoví, že N je složené. Pokud je splněna podmínka pro každé takové a, algoritmus odpoví, že N je asi prvočíslo.

Je nenulová pravděpodobnost, že algoritmus odpoví, že N je asi prvočíslo, přestože ve skutečnosti je N složené. Podle předchozí věty je tato pravděpodobnost menší než 4^{-r}, kde r je počet testovaných a.

Test Rabina a Millera

Pro dané N algoritmus otestuje podmínku předchozí věty pro předem daný počet r náhodně zvolených celých čísel a splňujících $1 < a < N - 1$. Pokud pro některé takové a není podmínka splněna, algoritmus odpoví, že N je složené. Pokud je splněna podmínka pro každé takové a, algoritmus odpoví, že N je asi prvočíslo.

Je nenulová pravděpodobnost, že algoritmus odpoví, že N je asi prvočíslo, přestože ve skutečnosti je N složené. Podle předchozí věty je tato pravděpodobnost menší než 4^{-r}, kde r je počet testovaných a. Pro lepší představu tuto pravděpodobnost porovnejme s pravděpodobností výhry ve hře Sportka, ve které se volí 6 čísel z 49.

Test Rabina a Millera

Pro dané N algoritmus otestuje podmínku předchozí věty pro předem daný počet r náhodně zvolených celých čísel a splňujících $1 < a < N - 1$. Pokud pro některé takové a není podmínka splněna, algoritmus odpoví, že N je složené. Pokud je splněna podmínka pro každé takové a, algoritmus odpoví, že N je asi prvočíslo.

Je nenulová pravděpodobnost, že algoritmus odpoví, že N je asi prvočíslo, přestože ve skutečnosti je N složené. Podle předchozí věty je tato pravděpodobnost menší než 4^{-r}, kde r je počet testovaných a. Pro lepší představu tuto pravděpodobnost porovnejme s pravděpodobností výhry ve hře Sportka, ve které se volí 6 čísel z 49.

Zvolíme-li v algoritmu $r = 12$, je pravděpodobnost, že o složeném N odpoví algoritmus, že je N asi prvočíslo, menší, než že na první pokus vyhrajeme Sportku (tj. uhádneme všech 6 tažených čísel).

Test Rabina a Millera

Pro dané N algoritmus otestuje podmínku předchozí věty pro předem daný počet r náhodně zvolených celých čísel a splňujících $1 < a < N - 1$. Pokud pro některé takové a není podmínka splněna, algoritmus odpoví, že N je složené. Pokud je splněna podmínka pro každé takové a, algoritmus odpoví, že N je asi prvočíslo.

Je nenulová pravděpodobnost, že algoritmus odpoví, že N je asi prvočíslo, přestože ve skutečnosti je N složené. Podle předchozí věty je tato pravděpodobnost menší než 4^{-r}, kde r je počet testovaných a. Pro lepší představu tuto pravděpodobnost porovnejme s pravděpodobností výhry ve hře Sportka, ve které se volí 6 čísel z 49.

Zvolíme-li v algoritmu $r = 12$, je pravděpodobnost, že o složeném N odpoví algoritmus, že je N asi prvočíslo, menší, než že na první pokus vyhrajeme Sportku (tj. uhádneme všech 6 tažených čísel). A pro $r = 24$ je tato pravděpodobnost menší, než že Sportku vyhrajeme dvakrát ze dvou pokusů.

Jak tedy volit velká prvočísla pro RSA?

Můžeme tedy volit vhodně velká lichá čísla a podrobovat je testu Rabina a Millera, dokud tento test neodpoví, že naše číslo je asi prvočíslo.

Jak tedy volit velká prvočísla pro RSA?

Můžeme tedy volit vhodně velká lichá čísla a podrobovat je testu Rabina a Millera, dokud tento test neodpoví, že naše číslo je asi prvočíslo.

Přestože s velkou pravděpodobností bude odpověď testu pravdivá, pro použití v RSA potřebujeme jistotu.

Jak tedy volit velká prvočísla pro RSA?

Můžeme tedy volit vhodně velká lichá čísla a podrobovat je testu Rabina a Millera, dokud tento test neodpoví, že naše číslo je asi prvočíslo.

Přestože s velkou pravděpodobností bude odpověď testu pravdivá, pro použití v RSA potřebujeme jistotu.

Existují mírně pomalejší algoritmy, které jsou schopny prvočíselnost takového čísla dokázat.

Jak tedy volit velká prvočísla pro RSA?

Můžeme tedy volit vhodně velká lichá čísla a podrobovat je testu Rabina a Millera, dokud tento test neodpoví, že naše číslo je asi prvočíslo.

Přestože s velkou pravděpodobností bude odpověď testu pravdivá, pro použití v RSA potřebujeme jistotu.

Existují mírně pomalejší algoritmy, které jsou schopny prvočíselnost takového čísla dokázat. Přestože jejich základní myšlenky jsou také založeny na znalostech algebry, nebudeme se už jimi v tomto předmětu M2150 Algebra I zabývat.

Jak tedy volit velká prvočísla pro RSA?

Můžeme tedy volit vhodně velká lichá čísla a podrobovat je testu Rabina a Millera, dokud tento test neodpoví, že naše číslo je asi prvočíslo.

Přestože s velkou pravděpodobností bude odpověď testu pravdivá, pro použití v RSA potřebujeme jistotu.

Existují mírně pomalejší algoritmy, které jsou schopny prvočíselnost takového čísla dokázat. Přestože jejich základní myšlenky jsou také založeny na znalostech algebry, nebudeme se už jimi v tomto předmětu M2150 Algebra I zabývat. Případní zájemci se o těchto algoritmech mohou dozvědět více v navazujícím předmětu M8190 Algoritmy teorie čísel.