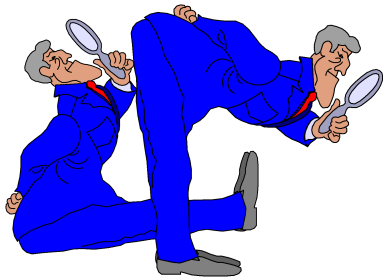
Kryptografie včera, dnes a zítra

Jan Paseka

Ústav matematiky a statistiky
Masarykova univerzita

13. září 2021

O čem to bude



Základní pojmy I

- ***Kryptologie*** - věda zabývající se šiframi.

Základní pojmy I

- ***Kryptologie*** - věda zabývající se šiframi.
- ***Kryptografie*** - část kryptologie zabývající se převedením srozumitelné zprávy do nesrozumitelné podoby a zpět (šifrování a dešifrování textu).

Základní pojmy I

- ***Kryptologie*** - věda zabývající se šiframi.
- ***Kryptografie*** - část kryptologie zabývající se převedením srozumitelné zprávy do nesrozumitelné podoby a zpět (šifrování a dešifrování textu).
- ***Kryptoanalýza*** - část kryptologie zabývající se odhalením klíče, čili umožněním čtení zašifrované zprávy.

Základní pojmy II

- ***Šifrování (encryption)*** - proces, při kterém převedeme podle určených pravidel otevřený text na šifrový text (cipher text).

Základní pojmy II

- ***Šifrování (encryption)*** - proces, při kterém převedeme podle určených pravidel otevřený text na šifrový text (cipher text).
- ***Dešifrování (decryption)*** - opačný proces k šifrování.

Základní pojmy II

- ***Šifrování (encryption)*** - proces, při kterém převedeme podle určených pravidel otevřený text na šifrový text (cipher text).
- ***Dešifrování (decryption)*** - opačný proces k šifrování.
- ***Klíč*** - posloupnost znaků, může být rozdílný pro šifrování a dešifrování.

Základní pojmy II

- ***Šifrování (encryption)*** - proces, při kterém převedeme podle určených pravidel otevřený text na šifrový text (cipher text).
- ***Dešifrování (decryption)*** - opačný proces k šifrování.
- ***Klíč*** - posloupnost znaků, může být rozdílný pro šifrování a dešifrování.
- ***Útok na šifru, lámání šifry*** - zkoušení všech možných klíčů.

Proč šifrovat? I

- ***Bankovnictví***

Proč šifrovat? I

- ***Bankovnictví***
- ***Veřejná správa***

Proč šifrovat? I

- ***Bankovnictví***
- ***Veřejná správa***
- ***Multimédia – DVD, CD, SAT TV***

Proč šifrovat? I

- ***Bankovnictví***
- ***Veřejná správa***
- ***Multimédia – DVD, CD, SAT TV***
- ***Firemní korespondence, obyčejný mail = pohlednice***

Proč šifrovat? I

- ***Bankovnictví***
- ***Veřejná správa***
- ***Multimédia – DVD, CD, SAT TV***
- ***Firemní korespondence, obyčejný mail = pohlednice***
- ***Odchozí dráty, routery, SMTP servery, POP3 server***

Proč šifrovat? I

- ***Bankovnictví***
- ***Veřejná správa***
- ***Multimédia – DVD, CD, SAT TV***
- ***Firemní korespondence, obyčejný mail = pohlednice***
- ***Odchozí dráty, routery, SMTP servery, POP3 server***
- ***Konkurence, váš obchodní partner, znuděný hacker, admin, který dostal výpověď, někdo, koho jste naštval***

Proč šifrovat? I

- ***Bankovnictví***
- ***Veřejná správa***
- ***Multimédia – DVD, CD, SAT TV***
- ***Firemní korespondence, obyčejný mail = pohlednice***
- ***Odchozí dráty, routery, SMTP servery, POP3 server***
- ***Konkurence, váš obchodní partner, znuděný hacker, admin, který dostal výpověď, někdo, koho jste naštval***
- ***Vyzrazení dat, modifikace dat***

Proč šifrovat? I

- ***Bankovnictví***
- ***Veřejná správa***
- ***Multimédia – DVD, CD, SAT TV***
- ***Firemní korespondence, obyčejný mail = pohlednice***
- ***Odchozí dráty, routery, SMTP servery, POP3 server***
- ***Konkurence, váš obchodní partner, znuděný hacker, admin, který dostal výpověď, někdo, koho jste naštval***
- ***Vyzrazení dat, modifikace dat***

Pokud je tajnost zprávy závislá na utajení algoritmu šifrování, je to ***VŽDY špatně.***

Proč šifrovat? I

- ***Bankovnictví***
- ***Veřejná správa***
- ***Multimédia – DVD, CD, SAT TV***
- ***Firemní korespondence, obyčejný mail = pohlednice***
- ***Odchozí dráty, routery, SMTP servery, POP3 server***
- ***Konkurence, váš obchodní partner, znuděný hacker, admin, který dostal výpověď, někdo, koho jste naštval***
- ***Vyzrazení dat, modifikace dat***

Pokud je tajnost zprávy závislá na utajení algoritmu šifrování, je to ***VŽDY špatně.***

Současné algoritmy šifrování jsou obecně známé a tajnost zprávy závisí pouze na tajnosti klíče.

Proč šifrovat? II

- ***Kryptologie***, která byla dříve výsadou tajných služeb, armád a diplomacie, se stává během v současnosti věcí veřejnou a současně i výnosným obchodem.

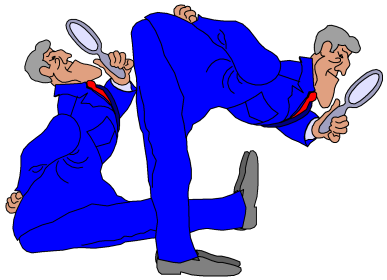
Proč šifrovat? II

- ***Kryptologie***, která byla dříve výsadou tajných služeb, armád a diplomacie, se stává během v současnosti věcí veřejnou a současně i výnosným obchodem.
- Zahajuje svoje masové tažení za ***všemi uživateli*** výpočetní techniky.

Proč šifrovat? II

- ***Kryptologie***, která byla dříve výsadou tajných služeb, armád a diplomacie, se stává během v současnosti věcí veřejnou a současně i výnosným obchodem.
- Zahajuje svoje masové tažení za ***všemi uživateli*** výpočetní techniky.
- Pojmy jako ***státní informační systém, e-business, e-commerce, e-obchodování, elektronický notář, kvalifikovaný certifikát, ochrana osobních dat a další*** se stávají samozřejmou součástí našeho jazyka a jejich realizace je možná právě díky kvalitním kryptografickým produktům a právnímu zajištění.

O čem to bude



Nejstarší šifry - Starověk

- ***Prvopočátky kryptografie před 4000 lety*** - použití nestandardních hieroglyfů ve starověkém Egyptě.

Nejstarší šifry - Starověk

- ***Prvopočátky kryptografie před 4000 lety*** - použití nestandardních hieroglyfů ve starověkém Egyptě.
- ***1 000 př. n. l. – ATBASH*** - jednoduchá substituční šifra

Prvních 13 písmen:	A	B	C	D	E	F	G	H	I	J	K	L	M
Posledních 13 písmen:	Z	Y	X	W	V	U	T	S	R	Q	P	O	N

Nejstarší šifry - Starověk

- ***Prvopočátky kryptografie před 4000 lety*** - použití nestandardních hieroglyfů ve starověkém Egyptě.
- ***1 000 př. n. l. – ATBASH*** - jednoduchá substituční šifra

Prvních 13 písmen:	A	B	C	D	E	F	G	H	I	J	K	L	M
Posledních 13 písmen:	Z	Y	X	W	V	U	T	S	R	Q	P	O	N

- ***Skytála (transpoziční šifra)***

Nejstarší šifry - Starověk

- ***Prvopočátky kryptografie před 4000 lety*** - použití nestandardních hieroglyfů ve starověkém Egyptě.
- ***1 000 př. n. l. – ATBASH*** - jednoduchá substituční šifra

Prvních 13 písmen:	A	B	C	D	E	F	G	H	I	J	K	L	M
Posledních 13 písmen:	Z	Y	X	W	V	U	T	S	R	Q	P	O	N

- ***Skytála (transpoziční šifra)***
  Před 2500 lety používala vláda ve Spartě následující metodu pro přenos tajné zprávy pro své generály: odesilatel a příjemce museli mít oba tzv. skytálu:

Nejstarší šifry - Starověk

- ***Prvopočátky kryptografie před 4000 lety*** - použití nestandardních hieroglyfů ve starověkém Egyptě.
- ***1 000 př. n. l. – ATBASH*** - jednoduchá substituční šifra

Prvních 13 písmen:	A	B	C	D	E	F	G	H	I	J	K	L	M
Posledních 13 písmen:	Z	Y	X	W	V	U	T	S	R	Q	P	O	N

- ***Skytála (transpoziční šifra)***
  Před 2500 lety používala vláda ve Spartě následující metodu pro přenos tajné zprávy pro své generály: odesilatel a příjemce museli mít oba tzv. skytálu: byly to dva válce o přesně stejném průměru.

Nejstarší šifry - Starověk

- ***Prvopočátky kryptografie před 4000 lety*** - použití nestandardních hieroglyfů ve starověkém Egyptě.
- ***1 000 př. n. l. – ATBASH*** - jednoduchá substituční šifra

Prvních 13 písmen:	A	B	C	D	E	F	G	H	I	J	K	L	M
Posledních 13 písmen:	Z	Y	X	W	V	U	T	S	R	Q	P	O	N

- ***Skytála (transpoziční šifra)***
  Před 2500 lety používala vláda ve Spartě následující metodu pro přenos tajné zprávy pro své generály: odesilatel a příjemce museli mít oba tzv. skytálu: byly to dva válce o přesně stejném průměru. Odesilatel navinul úzkou pergamenovou pásku spirálovitě okolo své skytály a napsal pak podle délky svou zprávu na pásku. Po odmotání pásky mohla zprávu číst jen ta osoba, která měla skytálu stejného rozměru –

Nejstarší šifry - Starověk

- ***Prvopočátky kryptografie před 4000 lety*** - použití nestandardních hieroglyfů ve starověkém Egyptě.
- ***1 000 př. n. l. – ATBASH*** - jednoduchá substituční šifra

Prvních 13 písmen:	A	B	C	D	E	F	G	H	I	J	K	L	M
Posledních 13 písmen:	Z	Y	X	W	V	U	T	S	R	Q	P	O	N

- ***Skytála (transpoziční šifra)***
  Před 2500 lety používala vláda ve Spartě následující metodu pro přenos tajné zprávy pro své generály: odesilatel a příjemce museli mít oba tzv. skytálu: byly to dva válce o přesně stejném průměru. Odesilatel navinul úzkou pergamenovou pásku spirálovitě okolo své skytály a napsal pak podle délky svou zprávu na pásku. Po odmotání pásky mohla zprávu číst jen ta osoba, která měla skytálu stejného rozměru – doufejme, že to byl pouze příjemce.

Nejstarší šifry - Starověk

- ***Caesarova šifra*** (posouvací šifry) - římský vojevůdce a státník Gaius Julius Caesar (100-44 př. n. l.).

Nejstarší šifry - Starověk

- ***Caesarova šifra*** (posouvací šifry) - římský vojevůdce a státník Gaius Julius Caesar (100-44 př. n. l.).
  Existují také Caesarovy dopisy Cicerovi a známým o věcech, v kterých psal tajným písmem, pokud něco muselo být důvěrně sděleno. Tzn. změnil pořadí písmen tak, že nešlo zjistit jediné slovo. Pokud někdo chtěl toto rozluštit apoznat obsah, musel dosadit čtvrté písmeno abecedy, tedy D, za A, a podobně toto provést se zbývajícími písmeny.

Nejstarší šifry - Starověk

- ***Caesarova šifra*** (posouvací šifry) - římský vojevůdce a státník Gaius Julius Caesar (100-44 př. n. l.).
  Existují také Caesarovy dopisy Cicerovi a známým o věcech, v kterých psal tajným písmem, pokud něco muselo být důvěrně sděleno. Tzn. změnil pořadí písmen tak, že nešlo zjistit jediné slovo. Pokud někdo chtěl toto rozluštit apoznat obsah, musel dosadit čtvrté písmeno abecedy, tedy D, za A, a podobně toto provést se zbývajícími písmeny.
  My můžeme ale posunout abecedu o libovolný možný počet míst. Protože se naše abeceda sestává z 26 písmen, existuje právě 26 takových šifrování - mluvíme o posouvacích neboli aditivních šifrách.

Arabští matematikové

- ***Abú Bakr Ahmad ben ‘Ali ben Wahshiyya an-Nabati*** publikoval několik šifrovacích abeced tradičně používaných v magii.

Arabští matematikové

- ***Abú Bakr Ahmad ben ‘Ali ben Wahshiyya an-Nabati*** publikoval několik šifrovacích abeced tradičně používaných v magii.
- ***1412 - encyklopedie Subh al-á sha***:
  Arabové byli první, kdo objevili a popsali metody kryptoanalýzy. Souhrn arabských poznatků je uveden v jednom oddíle ("Utajování tajných zpráv v dopisech") rozsáhlé čtrnáctidílné encyklopedie Subh al-á sha, která byla dokončena r. 1412.

Středověk – Evropa

- ***Albertiho disk*** (dva měděné kotouče, jeden o něco větší než druhý) - použití dvou šifrových abeced namísto jedné.
- ***1500 - první evropská kniha o šifrování, autor Johannes Trithemius*** - Poligraphia.
- ***Francois Viete (1540 - 1610)*** - Dešifroval pro francouzského krále Jindřicha IV. Navarrského španělské depeše. Byl nařčen ze spojení s ďáblem, protože použité šifrovací kódy byly považovány za nerozluštitelné.
- ***Giovanni Battista della Porta (1541 - 1615)*** - V roce 1583 publikoval práci o tajných kódech De furtivis literarum notis, kde popsal substituční šifru.
- ***Kardinál Richelieu*** - Přeskupoval písmena v textu pomocí klíčového slova, které definovalo změnu pozice písmen.

David Kahn: Codebreakers, Macmillan Co., New York 1967

Telegraf a vysílačky I

V současnosti leží hlavní úloha kryptografie v utajování elektronické komunikace. Krátce poté, co Samuel F. B. Morse v roce 1845 veřejně předvedl telegraf, objevily se obavy před vyzrazením posílaných zpráv. Co se stane, kdyby někdo zcizil telegrafní pásku? Co zabrání nepoctivému telegrafnímu úředníkovi ve zkopírování zprávy a jejímu případnému vyzrazení?

Telegraf a vysílačky I

V současnosti leží hlavní úloha kryptografie v utajování elektronické komunikace. Krátce poté, co Samuel F. B. Morse v roce 1845 veřejně předvedl telegraf, objevily se obavy před vyzrazením posílaných zpráv. Co se stane, kdyby někdo zcizil telegrafní pásku? Co zabrání nepoctivému telegrafnímu úředníkovi ve zkopírování zprávy a jejímu případnému vyzrazení?

Odpověd spočívala v kódování tajným kódem, který nemohl rozluštit nikdo jiný než oprávěný příjemce. Význam kryptografie dále stoupl s objevem radiové komunikace a s jejím použitím ve válkách. Bez použití kryptografie by mohl nepřítel velmi snadno zachytit zprávy, vysílané z fronty nebo na frontu.

Telegraf a vysílačky II

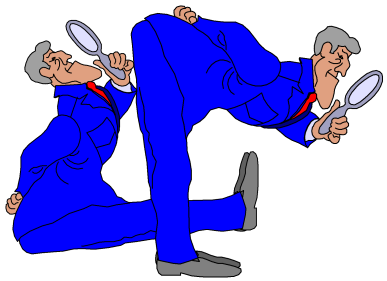
Vstup USA do I. světové války byl důsledkem vyluštění obsahu šifrového telegramu – dnes známého jako tzv. ***Zimmermannův telegram***, kde německý ministr zahraničí Zimmermann v telegramu mexické vládě vyzývá Mexiko k válce proti USA. Slibuje v ní mexické straně podporu a územní zisk.

Telegraf a vysílačky II

Vstup USA do I. světové války byl důsledkem vyluštění obsahu šifrového telegramu – dnes známého jako tzv. ***Zimmermannův telegram***, kde německý ministr zahraničí Zimmermann v telegramu mexické vládě vyzývá Mexiko k válce proti USA. Slibuje v ní mexické straně podporu a územní zisk.

Britové telegram zachytili, rozluštili jej a předali USA. Poté, co se prezident Wilson s obsahem telegramu seznámil, svolává Kongres. Ten 2.4.1917 schvaluje vstup USA do války proti Německu. Tento akt rozhodujícím způsobem změnil poměr sil na evropském bojišti.

O čem to bude



Vernamova šifra

Je to asi jediná šifrovací metoda, jejíž ***bezpečnost je matematicky dokazatelná***. Její princip spočívá v tom, že se ***zpráva*** zakóduje pomocí stejně dlouhé náhodné posloupnosti (klíče), čímž ***získá charakter zcela náhodného sledu znaků***.

Vernamova šifra

Je to asi jediná šifrovací metoda, jejíž ***bezpečnost je matematicky dokazatelná***. Její princip spočívá v tom, že se ***zpráva*** zakóduje pomocí stejně dlouhé náhodné posloupnosti (klíče), čímž ***získá charakter zcela náhodného sledu znaků***.

Takový klíč může být pochopitelně použit ***pouze jednou*** (proto se této metodě v angličtině říká také ***one time pad***) a musí být skutečně náhodný a nekorelovaný. Bez znalosti klíče nelze zprávu rozluštit.

Vernamova šifra

Je to asi jediná šifrovací metoda, jejíž ***bezpečnost je matematicky dokazatelná***. Její princip spočívá v tom, že se ***zpráva*** zakóduje pomocí stejně dlouhé náhodné posloupnosti (klíče), čímž ***získá charakter zcela náhodného sledu znaků***.

Takový klíč může být pochopitelně použit ***pouze jednou*** (proto se této metodě v angličtině říká také ***one time pad***) a musí být skutečně náhodný a nekorelovaný. Bez znalosti klíče nelze zprávu rozluštit.

Jinými slovy, ***pravděpodobnosti všech možných výsledků jsou stejné***. Neoprávněný luštitel má stejnou šanci dostat Shakespearovy sonety jako třeba daňové zákony. Opakované použití klíče nebo jeho části, či jakákoli pravidelnost v něm mohou dát luštitelům určitou šanci.

Vernamova šifra

Jak šifrování a dešifrování probíhá, ukazuje následující jednoduchý příklad. Používáme-li např. abecedu o 26 znacích, potřebujeme jako klíč sekvenci náhodných čísel z intervalu 0 až 25 (odesílatel i příjemce musí mít pochopitelně stejný klíč). Při šifrování se prostě posuneme v abecedě o patřičný počet míst (daný odpovídající hodnotou klíče) vpřed, při dešifrování vzad.

Vernamova šifra

Jak šifrování a dešifrování probíhá, ukazuje následující jednoduchý příklad. Používáme-li např. abecedu o 26 znacích, potřebujeme jako klíč sekvenci náhodných čísel z intervalu 0 až 25 (odesílatel i příjemce musí mít pochopitelně stejný klíč). Při šifrování se prostě posuneme v abecedě o patřičný počet míst (daný odpovídající hodnotou klíče) vpřed, při dešifrování vzad.

V případě binárně kódované zprávy je situace ještě jednodušší. Klíč má podobu náhodné posloupnosti nul a jedniček (stejně dlouhé, jako je zpráva), kterou můžeme získat třeba házením mincí. Při šifrování i dešifrování se bity zprávy a klíče jednoduše sečtou modulo 2 (operace XOR).

Vernamova šifra - příklad

Alice (encryption)

K: 1 0 1 1 0 0 1 0 0 1
M: 0 0 1 0 1 1 0 1 0 1

C: 1 0 0 1 1 1 1 1 0 0

Bob (decryption)

K: 1 0 1 1 0 0 1 0 0 1
C: 1 0 0 1 1 1 1 1 0 0

M: 0 0 1 0 1 1 0 1 0 1

Šifrovací stroj Enigma

Tento stroj způsobil zavedení počítačů do kryptografie a je základním kamenem pro pochopení způsobu práce moderních šifrovacích programů.

Šifrovací stroj Enigma

Tento stroj způsobil zavedení počítačů do kryptografie a je základním kamenem pro pochopení způsobu práce moderních šifrovacích programů.
Enigmu vyvinul na počátku 20. století Arthur Scherbius a začala se používat v dobách 2. světové války.

Šifrovací stroj Enigma

Tento stroj způsobil zavedení počítačů do kryptografie a je základním kamenem pro pochopení způsobu práce moderních šifrovacích programů.
Enigmu vyvinul na počátku 20. století Arthur Scherbius a začala se používat v dobách 2. světové války.
Šifrovací stroj Enigma se skládal z baterie, tlačítka pro každé písmeno abecedy, žárovky pro každé písmeno abecedy tzv. „lampboardu“ a ze série otočných disků, takzvaných rotorů.
Před klávesnicí Enigmy leží ještě deska zvaná „plugboard“, což je ve skutečnosti 26 konektorů, pomocí kterých se mohou spojovat jednotlivá písmena, např. C na P apod.

Šifrovací stroj Enigma

Princip Enigmy odpovídal dětské hračce: po zmáčknutí tlačítka se rozsvítilo nějaké světýlko. Když se pootočily rotory, změnilo se přiřazení mezi tlačítky a světýlky.

Šifrovací stroj Enigma

Princip Enigmy odpovídal dětské hračce: po zmáčknutí tlačítka se rozsvítilo nějaké světýlko. Když se pootočily rotory, změnilo se přiřazení mezi tlačítky a světýlky.

Rotory byly rozhodující zařízení pro šifrovací schopnosti stroje. Každý rotor se tak trochu podobal sendviči s 52 kontakty na každé straně. Uvnitř rotoru bylo 52 drátků, z nichž každý spojoval dva kontakty na dvou stranách rotoru.

Šifrovací stroj Enigma

Princip Enigmy odpovídal dětské hračce: po zmáčknutí tlačítka se rozsvítilo nějaké světýlko. Když se pootočily rotory, změnilo se přiřazení mezi tlačítky a světýlky.

Rotory byly rozhodující zařízení pro šifrovací schopnosti stroje. Každý rotor se tak trochu podobal sendviči s 52 kontakty na každé straně. Uvnitř rotoru bylo 52 drátků, z nichž každý spojoval dva kontakty na dvou stranách rotoru.

Drátky ovšem nespojovaly odpovídající si kontakty na obou stranách, propojovaly je v rozházeném pořadí, takže například kontakt č. 1 na levé vnitřní straně rotoru byl spojen s kontaktem č. 15 na pravé vnitřní straně rotoru a podobně.

Šifrovací stroj Enigma

Enigma používala tři rotory za sebou. Na konci řady rotorů byl reflektor, který poslal elektrický signál zpět ke druhému průchodu strojem. (Na konci války používal systém se čtyřmi rotory.)

Šifrovací stroj Enigma

Enigma používala tři rotory za sebou. Na konci řady rotorů byl reflektor, který poslal elektrický signál zpět ke druhému průchodu strojem. (Na konci války používal systém se čtyřmi rotory.)

Polovina z 52 kontaktů byla napojena na tlačítka a baterii, druhá polovina byla připojena k žárovkám. Stisknutím každého tlačítka způsobilo uzavření obvodu a rozsvítila se určitá žárovka. Která žárovka se však rozsvítí, to záleželo na poloze všech tří rotorů a reflektoru.

Šifrovací stroj Enigma

Enigma používala tři rotory za sebou. Na konci řady rotorů byl reflektor, který poslal elektrický signál zpět ke druhému průchodu strojem. (Na konci války používal systém se čtyřmi rotory.)

Polovina z 52 kontaktů byla napojena na tlačítka a baterii, druhá polovina byla připojena k žárovkám. Stisknutím každého tlačítka způsobilo uzavření obvodu a rozsvítila se určitá žárovka. Která žárovka se však rozsvítí, to záleželo na poloze všech tří rotorů a reflektoru.

Při šifrování nebo dešifrování zprávy nastavil šifrér rotory do určité výchozí pozice - to byl klíč. Pro každé písmeno zprávy teď zmáčkl tlačítko, zapsal, které písmeno se rozsvítilo, a pootočil rotory.

Šifrovací stroj Enigma

Protože se rotory pootočily po každém znaku, bylo stejné písmeno vstupního textu obvykle zašifrováno vždy jako dvě jiná.

Šifrovací stroj Enigma

Protože se rotory pootočily po každém znaku, bylo stejné písmeno vstupního textu obvykle zašifrováno vždy jako dvě jiná.

Enigma tedy byla substituční stroj s jinou substitucí pro každý znak zprávy - tomuto druhu šifer se říká polyalfabetické šifry.

Šifrovací stroj Enigma

Protože se rotory pootočily po každém znaku, bylo stejné písmeno vstupního textu obvykle zašifrováno vždy jako dvě jiná.

Enigma tedy byla substituční stroj s jinou substitucí pro každý znak zprávy - tomuto druhu šifer se říká polyalfabetické šifry.

Namísto mezery se používalo písmeno Z, čísla se rozepisovala.

Šifrovací stroj Enigma

Protože se rotory pootočily po každém znaku, bylo stejné písmeno vstupního textu obvykle zašifrováno vždy jako dvě jiná.

Enigma tedy byla substituční stroj s jinou substitucí pro každý znak zprávy - tomuto druhu šifer se říká polyalfabetické šifry.

Namísto mezery se používalo písmeno Z, čísla se rozepisovala.

Dešifrování zprávy bez znalosti počáteční polohy rotorů bylo (v té době) velmi obtížné.

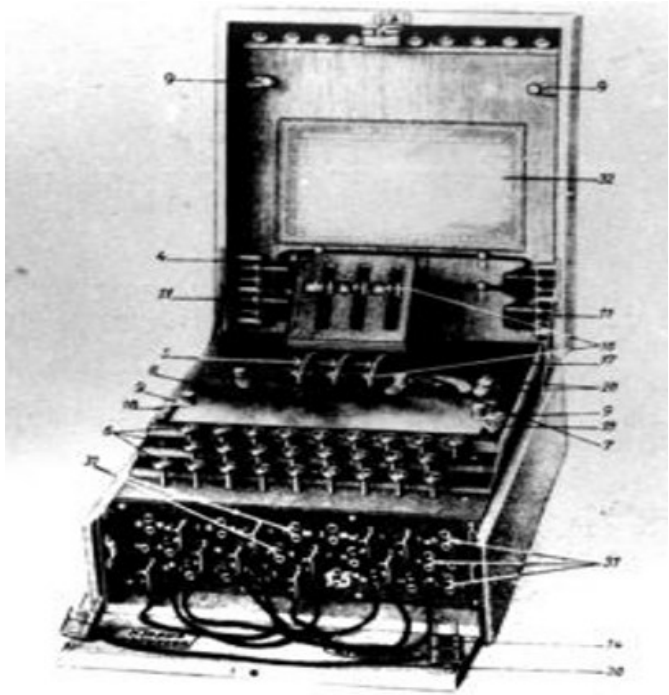
Šifrovací stroj Enigma

Protože se rotory pootočily po každém znaku, bylo stejné písmeno vstupního textu obvykle zašifrováno vždy jako dvě jiná.

Enigma tedy byla substituční stroj s jinou substitucí pro každý znak zprávy - tomuto druhu šifer se říká polyalfabetické šifry.

Namísto mezery se používalo písmeno Z, čísla se rozepisovala.

Dešifrování zprávy bez znalosti počáteční polohy rotorů bylo (v té době) velmi obtížné.



Code talkers

Code talkers byli američtí indiáni, kteří používali svůj kmenový jazyk k vysílání tajných sdělení na bojišti.

Code talkers

Code talkers byli američtí indiáni, kteří používali svůj kmenový jazyk k vysílání tajných sdělení na bojišti.

Většina lidí slyšela o indiánech kmene Navajo (nebo Diné), kteří používali svůj tradiční jazyk k přenosu tajných spojeneckých zpráv v tichomořském divadle boje během druhé světové války.

Code talkers

Code talkers byli američtí indiáni, kteří používali svůj kmenový jazyk k vysílání tajných sdělení na bojišti.

Většina lidí slyšela o indiánech kmene Navajo (nebo Diné), kteří používali svůj tradiční jazyk k přenosu tajných spojeneckých zpráv v tichomořském divadle boje během druhé světové války.

Ale nejméně 14 dalších domorodých národů sloužilo během války v Pacifiku i Evropě na této pozici. Myšlenka využití amerických indiánů, kteří plynně hovořili jak svým tradičním kmenovým jazykem, tak anglicky, k zasílání tajných zpráv v bitvě, byla poprvé testována v první světové válce s telefonním oddílem Choctaw a dalšími domorodými komunikačními odborníky a posly.

Code talkers

Code talkers byli američtí indiáni, kteří používali svůj kmenový jazyk k vysílání tajných sdělení na bojišti.

Většina lidí slyšela o indiánech kmene Navajo (nebo Diné), kteří používali svůj tradiční jazyk k přenosu tajných spojeneckých zpráv v tichomořském divadle boje během druhé světové války.

Ale nejméně 14 dalších domorodých národů sloužilo během války v Pacifiku i Evropě na této pozici. Myšlenka využití amerických indiánů, kteří plynně hovořili jak svým tradičním kmenovým jazykem, tak anglicky, k zasílání tajných zpráv v bitvě, byla poprvé testována v první světové válce s telefonním oddílem Choctaw a dalšími domorodými komunikačními odborníky a posly.

Až po druhé světové válce však americká armáda vyvinula specifickou politiku náboru a výcviku mluvčího indiánů, aby se

Code talkers

Americká armáda byla první, kdo začal přijímat code talkers v roce 1940. O několik let později následovaly námořní pěchota a námořnictvo USA. Prvních 29 code talkers v rámci Navajo US Marine dokončilo výcvik v roce 1942. Kromě základního výcviku museli tito muži vyvinout a zapamatovat si jedinečný vojenský kód pomocí svého převážně nepsaného jazyka.

Code talkers

Americká armáda byla první, kdo začal přijímat code talkers v roce 1940. O několik let později následovaly námořní pěchota a námořnictvo USA. Prvních 29 code talkers v rámci Navajo US Marine dokončilo výcvik v roce 1942. Kromě základního výcviku museli tito muži vyvinout a zapamatovat si jedinečný vojenský kód pomocí svého převážně nepsaného jazyka.

První typ kódu, který vytvořili, kód typu 1, se skládal z 26 výrazů Navajo, které zastupovaly jednotlivá anglická písmena, která bylo možné použít k hláskování slova. Například slovo Navajo pro „mravence“ wo-la-chee bylo použito k reprezentaci písmene „a“ v angličtině.

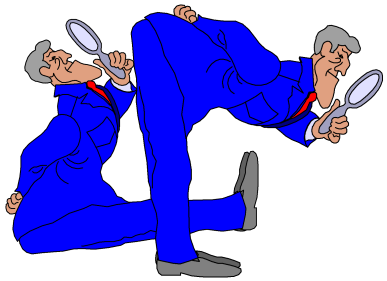
Code talkers

Americká armáda byla první, kdo začal přijímat code talkers v roce 1940. O několik let později následovaly námořní pěchota a námořnictvo USA. Prvních 29 code talkers v rámci Navajo US Marine dokončilo výcvik v roce 1942. Kromě základního výcviku museli tito muži vyvinout a zapamatovat si jedinečný vojenský kód pomocí svého převážně nepsaného jazyka.

První typ kódu, který vytvořili, kód typu 1, se skládal z 26 výrazů Navajo, které zastupovaly jednotlivá anglická písmena, která bylo možné použít k hláskování slova. Například slovo Navajo pro „mravence“ wo-la-chee bylo použito k reprezentaci písmene „a“ v angličtině.

Kód typu 2 obsahoval slova, která lze přímo přeložit z angličtiny do Navajo, a mluvčí kódu také vyvinuli slovník 211 výrazů (později rozšířených na 411) pro vojenská slova a jména, která původně v jazyce Navajo neexistovala.

O čem to bude



Claude Shannon

50.-60. léta rozvoj počítačů, kryptografie pro veřejnost (banky).

Claude Shannon

50.-60. léta rozvoj počítačů, kryptografie pro veřejnost (banky).

Tato epocha je charakteristická 2 pracemi od ***Claude Elwood Shannona***. V časopise Bell Systém Technical Journal v roce 1948 a 1949 otiskuje články ***Matematická teorie sdělování*** a ***Sdělovací teorie tajných systémů***.

Claude Shannon

50.-60. léta rozvoj počítačů, kryptografie pro veřejnost (banky).

Tato epocha je charakteristická 2 pracemi od ***Claude Elwood Shannona***. V časopise Bell Systém Technical Journal v roce 1948 a 1949 otiskuje články ***Matematická teorie sdělování*** a ***Sdělovací teorie tajných systémů***.

Prvý z článků dal vznik ***teorii informací***, druhý článek pojednával o kryptologii v termínech informační teorie. Pojetí ***nadbytečnosti (redundancy)*** je hlavním termínem, který Shannon zavedl.

DES

1973 - požadavky na algoritmus na ochranu neutajovaných dat

DES

1973 - požadavky na algoritmus na ochranu neutajovaných dat

DES - Data Encryption Standard: Tento algoritmus byl vyvinut firmou IBM a v roce ***1977*** se stal veřejným standard pro ochranu informací, nikoliv však pro ochranu informací utajovaných. DES nešifruje písmena, nýbrž symboly 0 a 1, a to 64 naráz (v případě, že používáme DES k zašifrování obyčejného textu, musí být písmena nejdřív přeložena do řetězce bitů.

Vývoj DES navazuje na vývoj šifrovacího algoritmu ***Lucifer*** od Thomase Watsona. Aktivní délka klíče je 56 bitů, hlavní prvky, které chrání šifrový text před útoky analytiků, jsou tzv. S-boxy. V roce 1976 byla uspořádána NBS (Národní úřad pro standardizaci) dvoudenní konference k diskuzi o DES.

DES

1973 - požadavky na algoritmus na ochranu neutajovaných dat

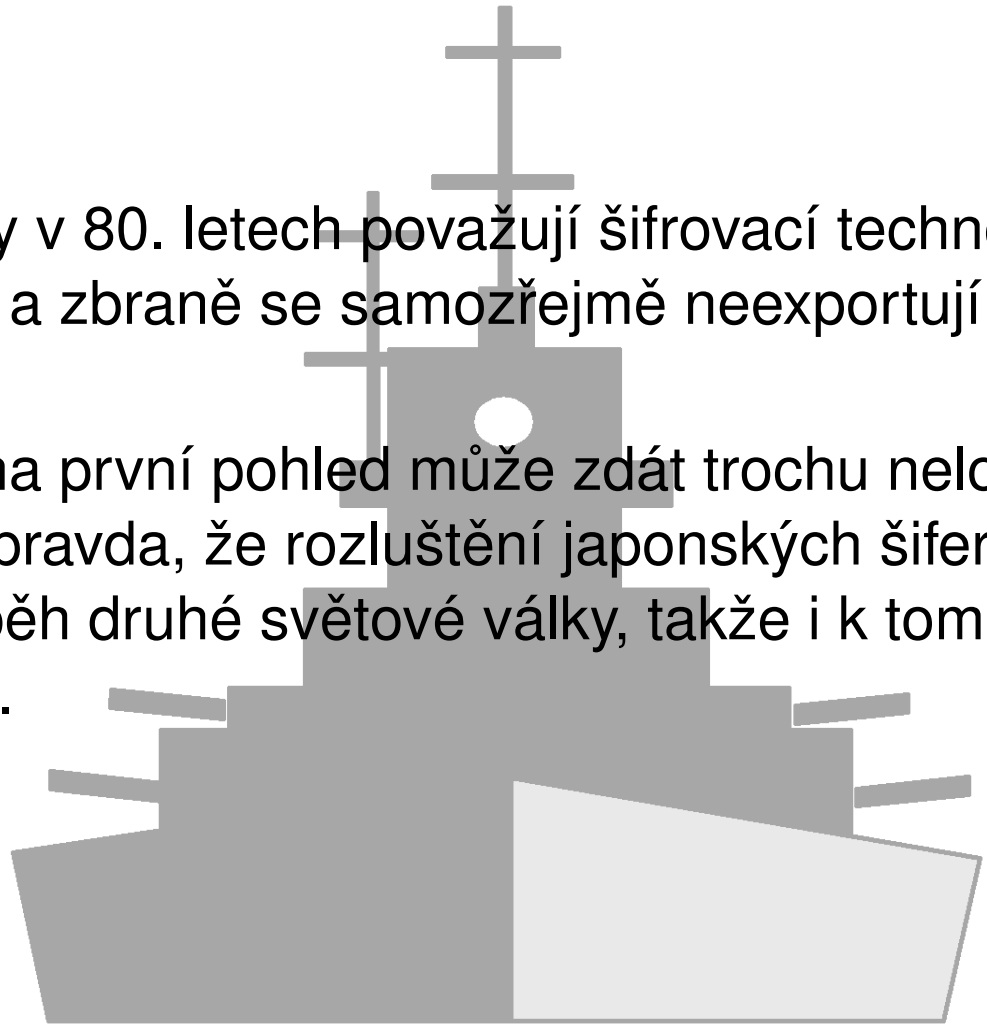
DES - Data Encryption Standard: Tento algoritmus byl vyvinut firmou IBM a v roce ***1977*** se stal veřejným standard pro ochranu informací, nikoliv však pro ochranu informací utajovaných. DES nešifruje písmena, nýbrž symboly 0 a 1, a to 64 naráz (v případě, že používáme DES k zašifrování obyčejného textu, musí být písmena nejdřív přeložena do řetězce bitů.
Vývoj DES navazuje na vývoj šifrovacího algoritmu ***Lucifer*** od Thomase Watsona. Aktivní délka klíče je 56 bitů, hlavní prvky, které chrání šifrový text před útoky analytiků, jsou tzv. S-boxy. V roce 1976 byla uspořádána NBS (Národní úřad pro standardizaci) dvoudenní konference k diskuzi o DES.

množství šifer (symetrické i asymetrické), PGP

Export šifer

Spojené státy v 80. letech považují šifrovací technologie za druh zbraně, a zbraně se samozřejmě neexportují jen tak ledaskam.

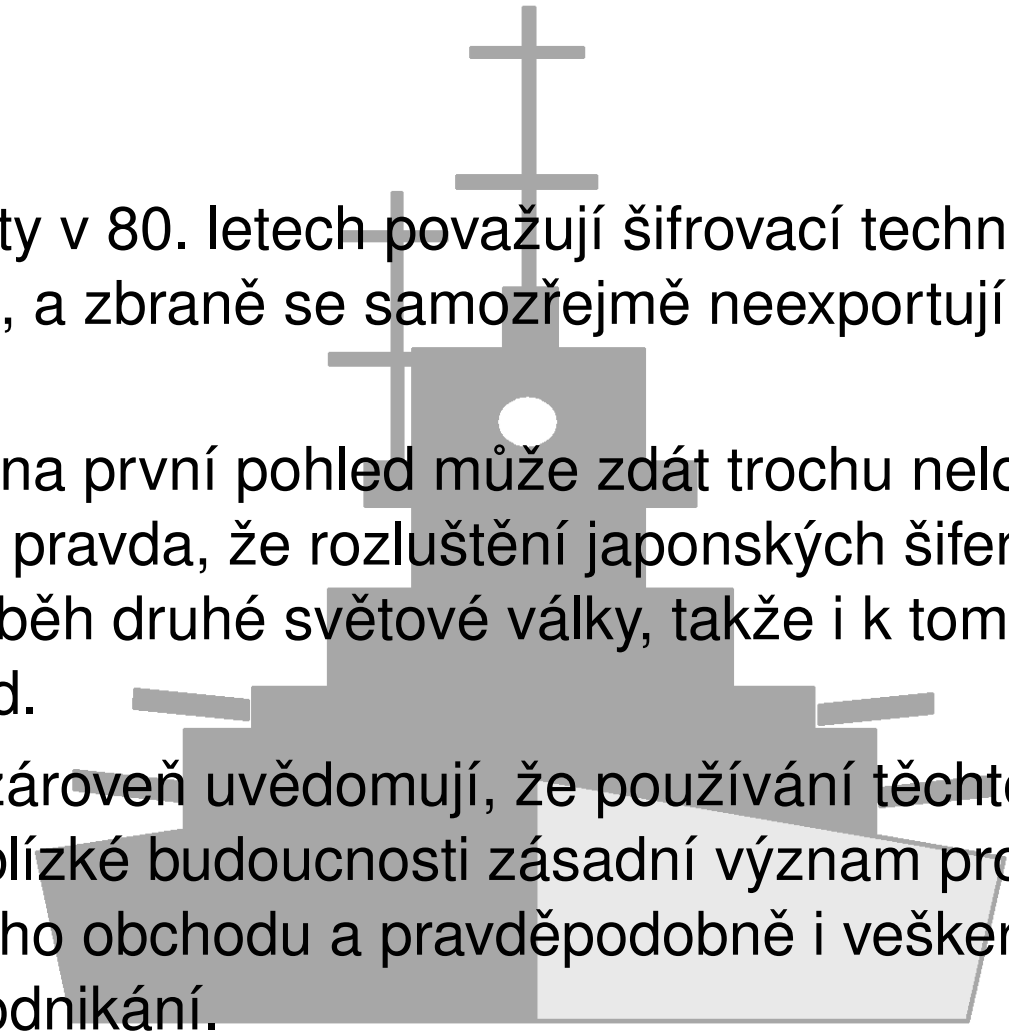
Export šifer



Spojené státy v 80. letech považují šifrovací technologie za druh zbraně, a zbraně se samozřejmě neexportují jen tak ledaskam.

I když se to na první pohled může zdát trochu nelogické, je koneckonců pravda, že rozluštění japonských šifer výrazně ovlivnilo průběh druhé světové války, takže i k tomu mají i pádný důvod.

Export šifer



Spojené státy v 80. letech považují šifrovací technologie za druh zbraně, a zbraně se samozřejmě neexportují jen tak ledaskam.

I když se to na první pohled může zdát trochu nelogické, je koneckonců pravda, že rozluštění japonských šifer výrazně ovlivnilo průběh druhé světové války, takže i k tomu mají i pádný důvod.

USA si ale zároveň uvědomují, že používání těchto technologií bude mít v blízké budoucnosti zásadní význam pro rozvoj elektronického obchodu a pravděpodobně i veškerého ostatního podnikání.

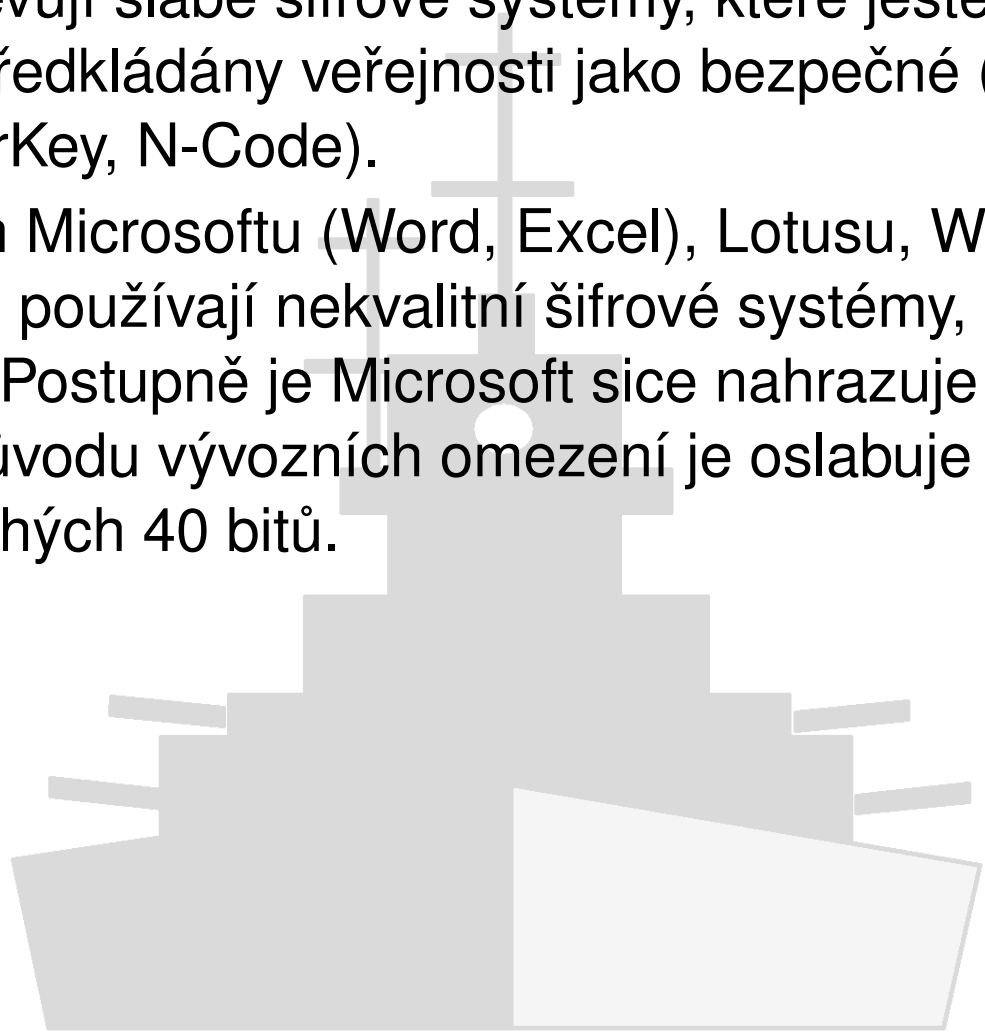
Export šifer - Zlomové roky 1999–2000

Již se neobjevují slabé šifrové systémy, které ještě v polovině 90. let byly předkládány veřejnosti jako bezpečné (např. Crypt, Rot13, SuperKey, N-Code).

Export šifer - Zlomové roky 1999–2000

Již se neobjevují slabé šifrové systémy, které ještě v polovině 90. let byly předkládány veřejnosti jako bezpečné (např. Crypt, Rot13, SuperKey, N-Code).

V produktech Microsoftu (Word, Excel), Lotusu, WordPerfectu se však stále používají nekvalitní šifrové systémy, které lze lehce rozbít. Postupně je Microsoft sice nahrazuje za kvalitní šifru, ale z důvodu vývozních omezení je oslabuje úpravou klíče na délku pouhých 40 bitů.



Export šifer - Zlomové roky 1999–2000

Již se neobjevují slabé šifrové systémy, které ještě v polovině 90. let byly předkládány veřejnosti jako bezpečné (např. Crypt, Rot13, SuperKey, N-Code).

V produktech Microsoftu (Word, Excel), Lotusu, WordPerfectu se však stále používají nekvalitní šifrové systémy, které lze lehce rozbít. Postupně je Microsoft sice nahrazuje za kvalitní šifru, ale z důvodu vývozních omezení je oslabuje úpravou klíče na délku pouhých 40 bitů.

Takto úmyslně upraveným algoritmům se říká ***slabá kryptografie***. Mimo území USA a Kanady se tak stále v těchto produktech nacházejí slabé šifrové produkty.

Export šifer - Zlomové roky 1999–2000

Již se neobjevují slabé šifrové systémy, které ještě v polovině 90. let byly předkládány veřejnosti jako bezpečné (např. Crypt, Rot13, SuperKey, N-Code).

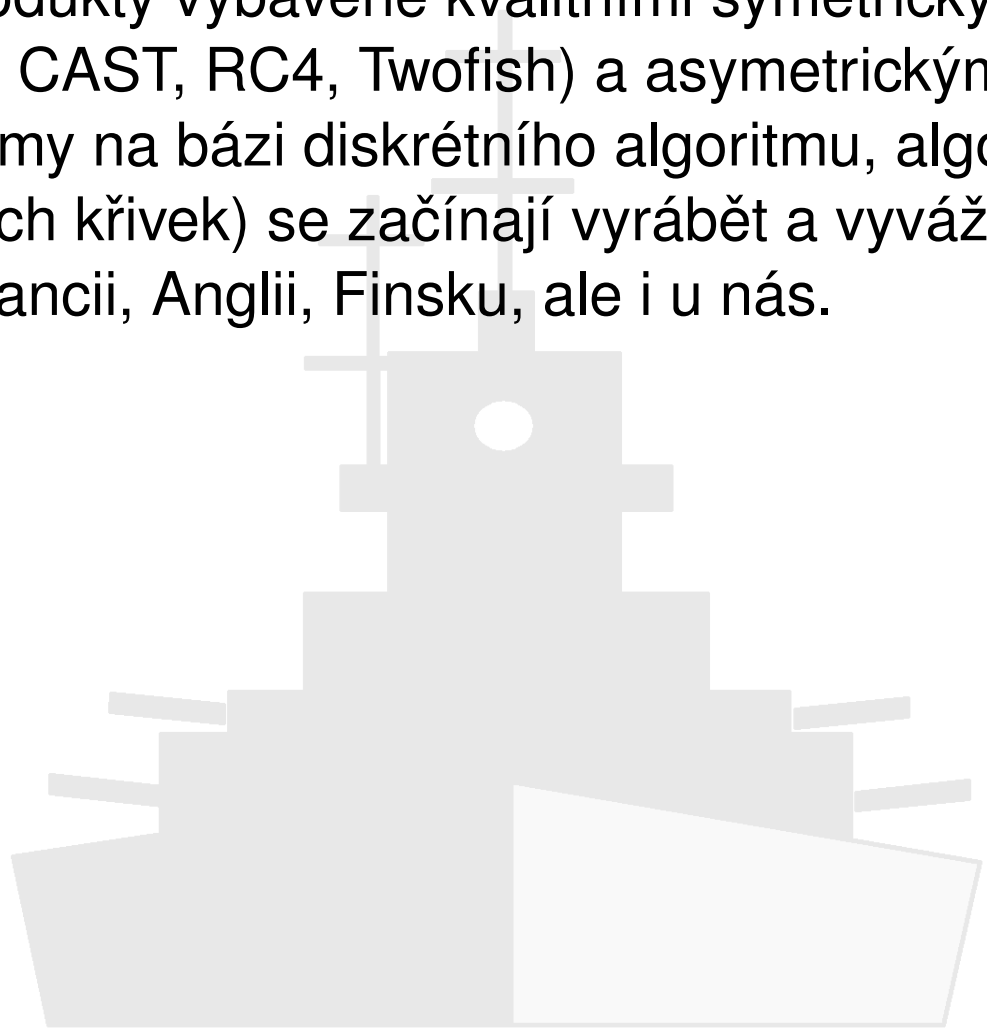
V produktech Microsoftu (Word, Excel), Lotusu, WordPerfectu se však stále používají nekvalitní šifrové systémy, které lze lehce rozbít. Postupně je Microsoft sice nahrazuje za kvalitní šifru, ale z důvodu vývozních omezení je oslabuje úpravou klíče na délku pouhých 40 bitů.

Takto úmyslně upraveným algoritmům se říká ***slabá kryptografie***. Mimo území USA a Kanady se tak stále v těchto produktech nacházejí slabé šifrové produkty.

Toto je ovšem výhodná situace pro evropské komerční firmy, které se snaží obsadit evropský trh svými produkty. Americké velké firmy se snaží donutit vládu USA k omezení vývozních restrikcí, ale ta neustupuje.

Export šifer - Zlomové roky 1999–2000

Komerční produkty vybavené kvalitními symetrickými algoritmy (např. 3DES, CAST, RC4, Twofish) a asymetrickými algoritmy (RSA, algoritmy na bázi diskrétního algoritmu, algoritmy na bázi eliptických křivek) se začínají vyrábět a vyvážet nejen v Německu, Francii, Anglii, Finsku, ale i u nás.



Export šifer - Zlomové roky 1999–2000

Komerční produkty vybavené kvalitními symetrickými algoritmy (např. 3DES, CAST, RC4, Twofish) a asymetrickými algoritmy (RSA, algoritmy na bázi diskrétního algoritmu, algoritmy na bázi eliptických křivek) se začínají vyrábět a vyvážet nejen v Německu, Francii, Anglii, Finsku, ale i u nás.

Česká firma Decros úspěšně vyváží své produkty nejen do Evropy, ale i do Asie. Květen 1999 je pro Českou republiku určitým ohodnocením naší vyspělosti v této oblasti. Výbor IACR v roce 1997 rozhodl, že konference Eurocrypt 1999 se bude konat v Praze.

Export šifer - Zlomové roky 1999–2000

Komerční produkty vybavené kvalitními symetrickými algoritmy (např. 3DES, CAST, RC4, Twofish) a asymetrickými algoritmy (RSA, algoritmy na bázi diskrétního algoritmu, algoritmy na bázi eliptických křivek) se začínají vyrábět a vyvážet nejen v Německu, Francii, Anglii, Finsku, ale i u nás.

Česká firma Decros úspěšně vyváží své produkty nejen do Evropy, ale i do Asie. Květen 1999 je pro Českou republiku určitým ohodnocením naší vyspělosti v této oblasti. Výbor IACR v roce 1997 rozhodl, že konference Eurocrypt 1999 se bude konat v Praze.

V létě 1999 německá vláda vydává prohlášení, ve kterém jasně proklamuje, že na dobu dvou let ruší všechny restrikce v používání silné kryptografie a dává celému světu najevo, že chce zaujmout rozhodující pozici v evropském trhu s kryptografií.

Export šifer - Zlomové roky 1999–2000

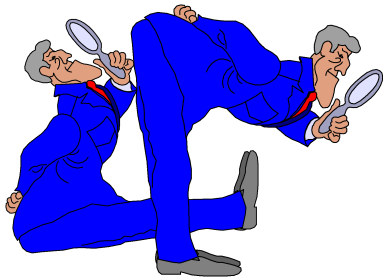
Tlak amerických firem, které přicházejí o miliony dolarů, nakonec slaví úspěch. V listopadu 1999 dochází k prvnímu uvolnění vývozních restrikcí a další uvolnění následuje v lednu 2000. S konečnou platností je tak uvolněn export šifrovacích algoritmů ze Spojených států (včetně zdrojových textů).

Export šifer - Zlomové roky 1999–2000

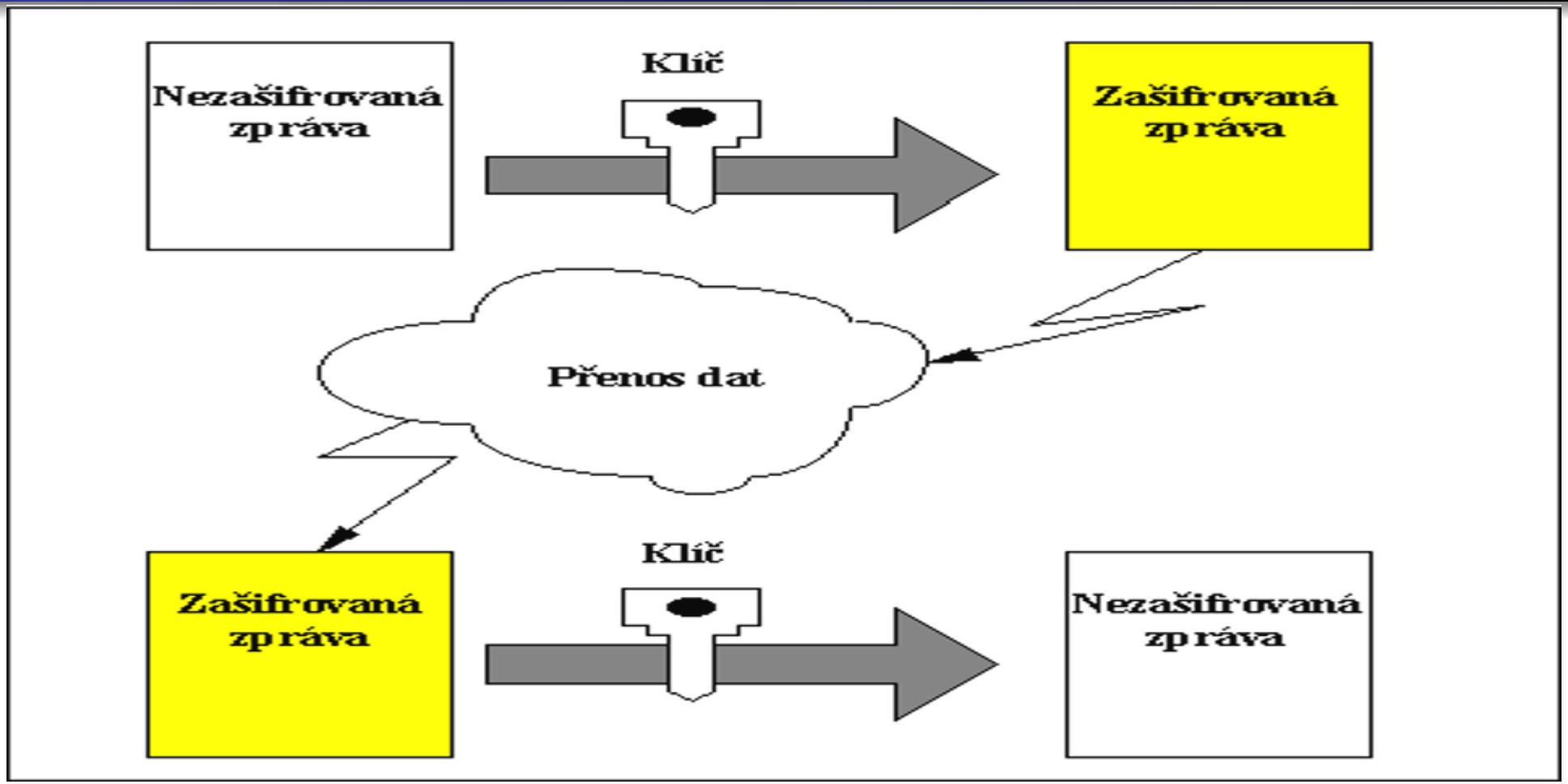
Tlak amerických firem, které přicházejí o miliony dolarů, nakonec slaví úspěch. V listopadu 1999 dochází k prvnímu uvolnění vývozních restrikcí a další uvolnění následuje v lednu 2000. S konečnou platností je tak uvolněn export šifrovacích algoritmů ze Spojených států (včetně zdrojových textů).

V lednu 2000 byl také zahájen 3 letý projekt NESSIE (New European Schemes for Signature, Integrity, and Encryption) programu IST Evropské komise. Jednotlivé moduly budou vytvářeny na základě veřejných návrhů a rovněž tak vyhodnocení těchto návrhů proběhne otevřenou a transparentní cestou.

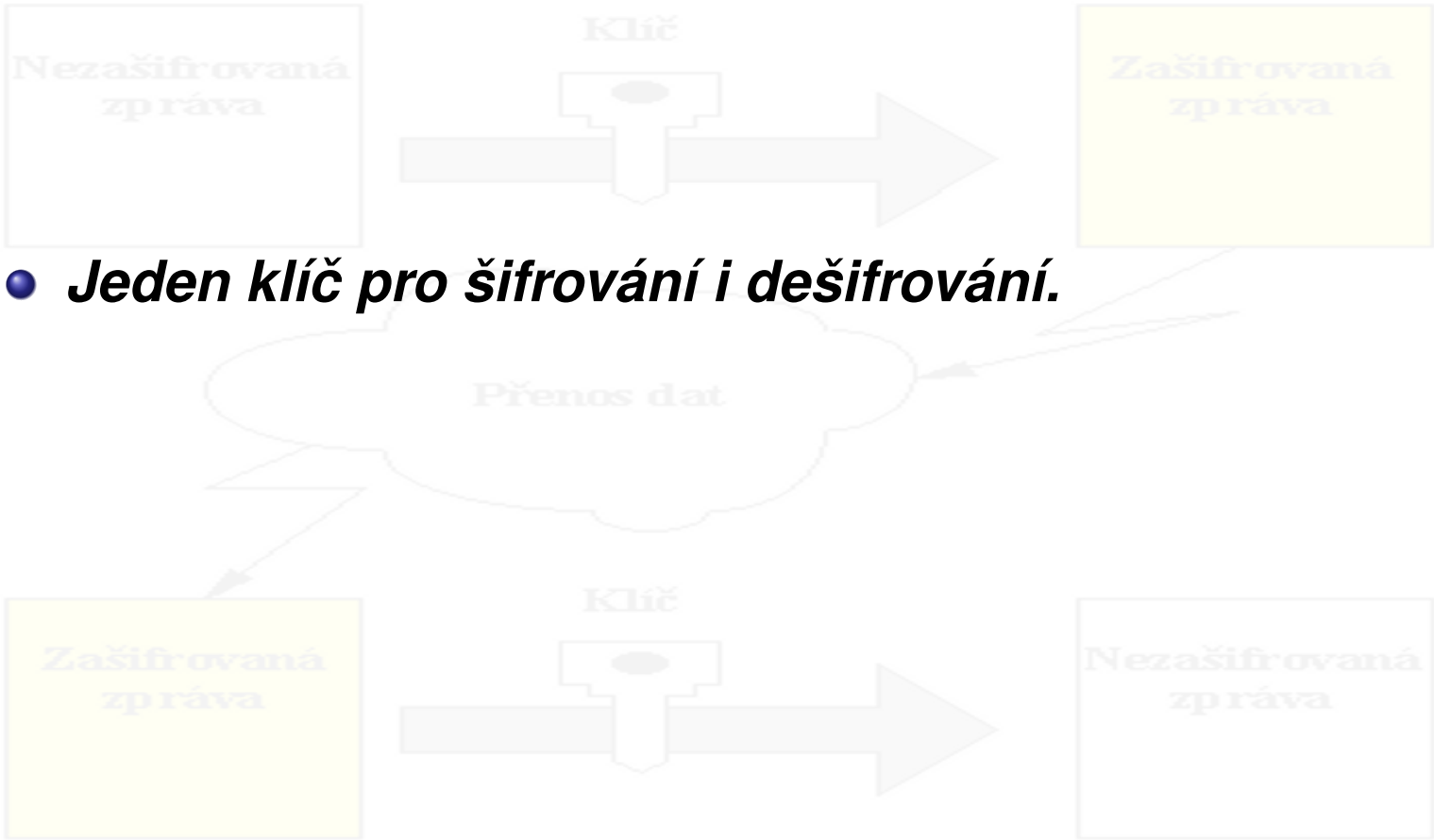
O čem to bude



Symetrické šifrování

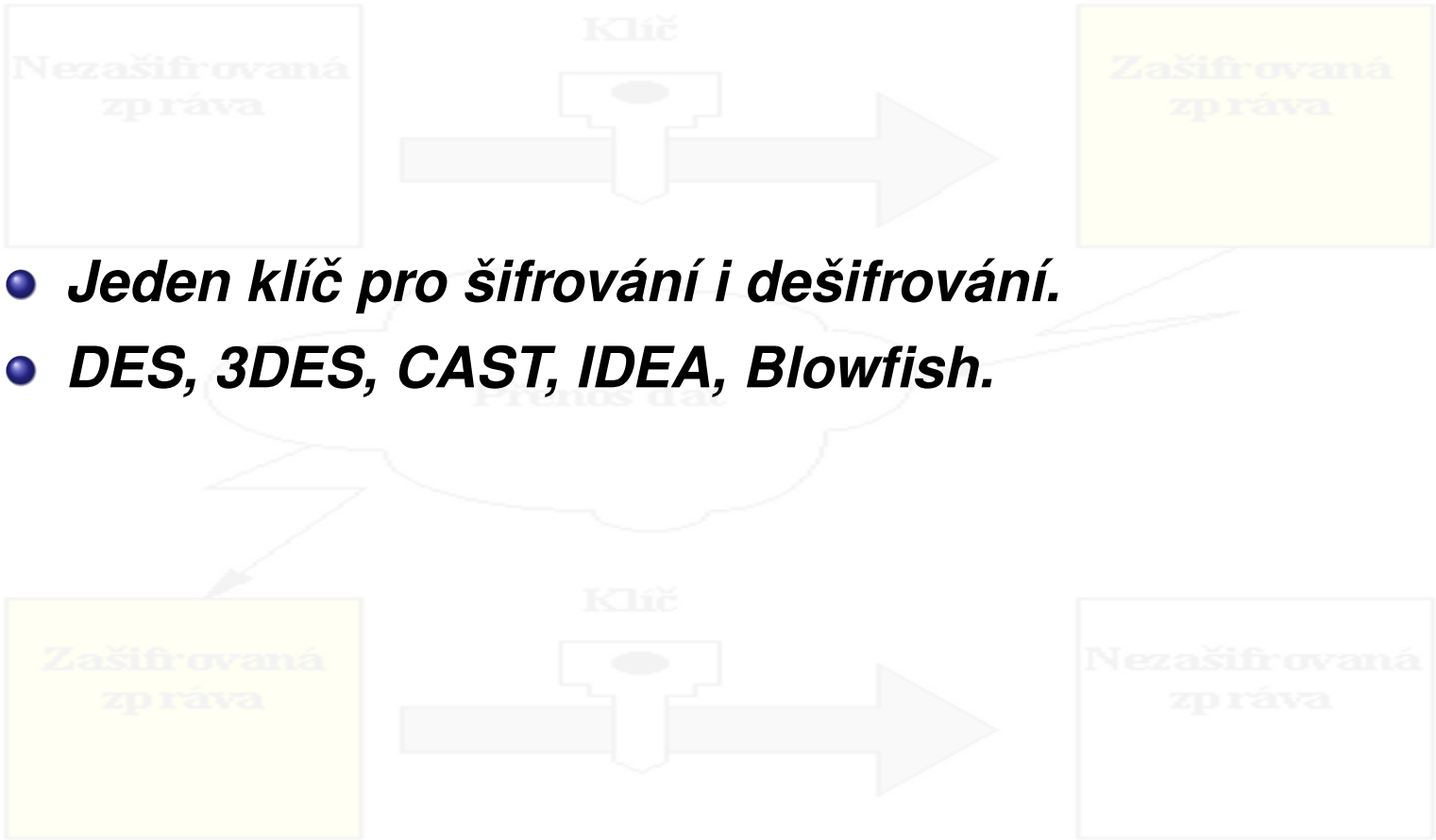


Symetrické šifrování



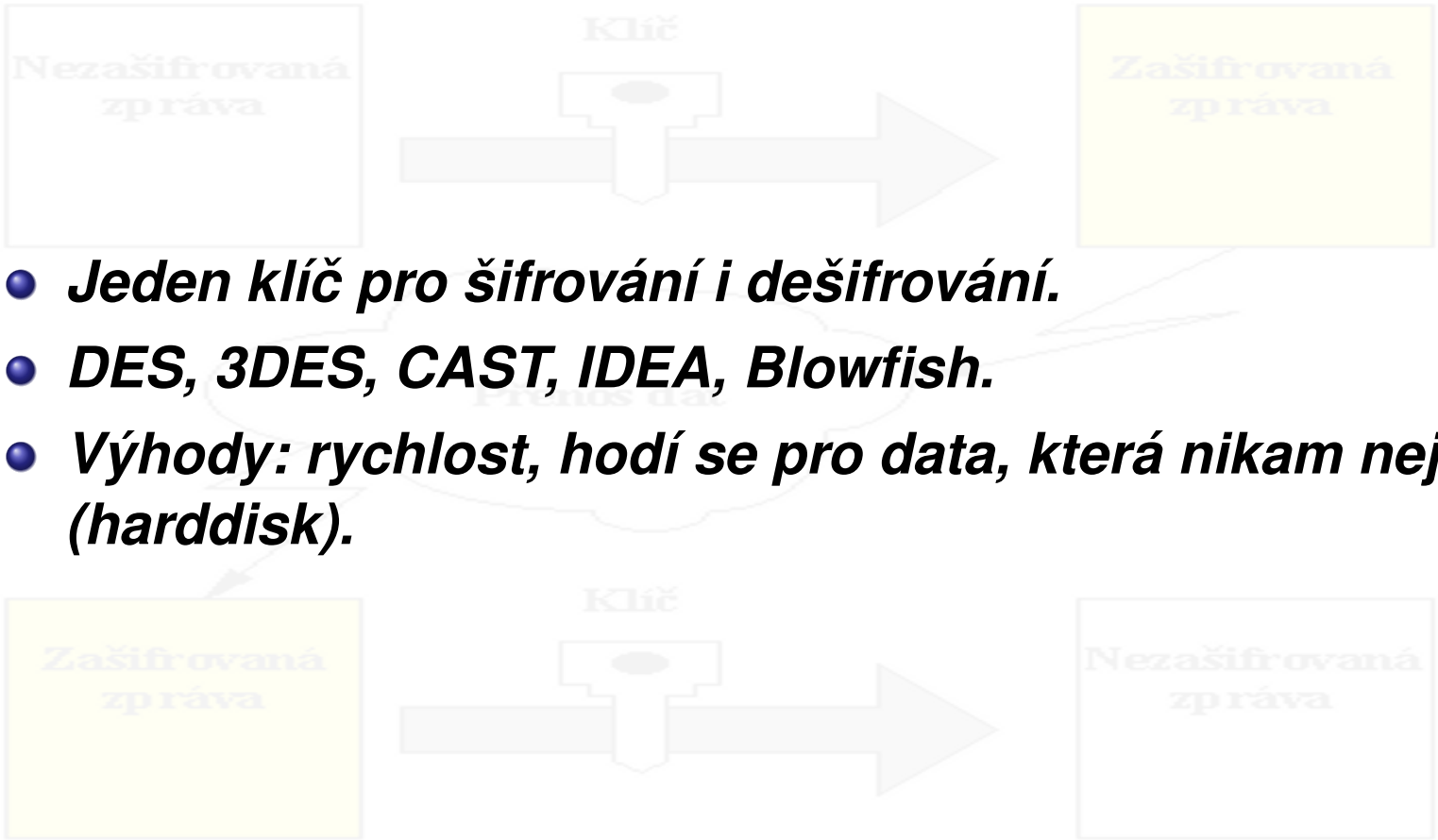
- ***Jeden klíč pro šifrování i dešifrování.***

Symetrické šifrování



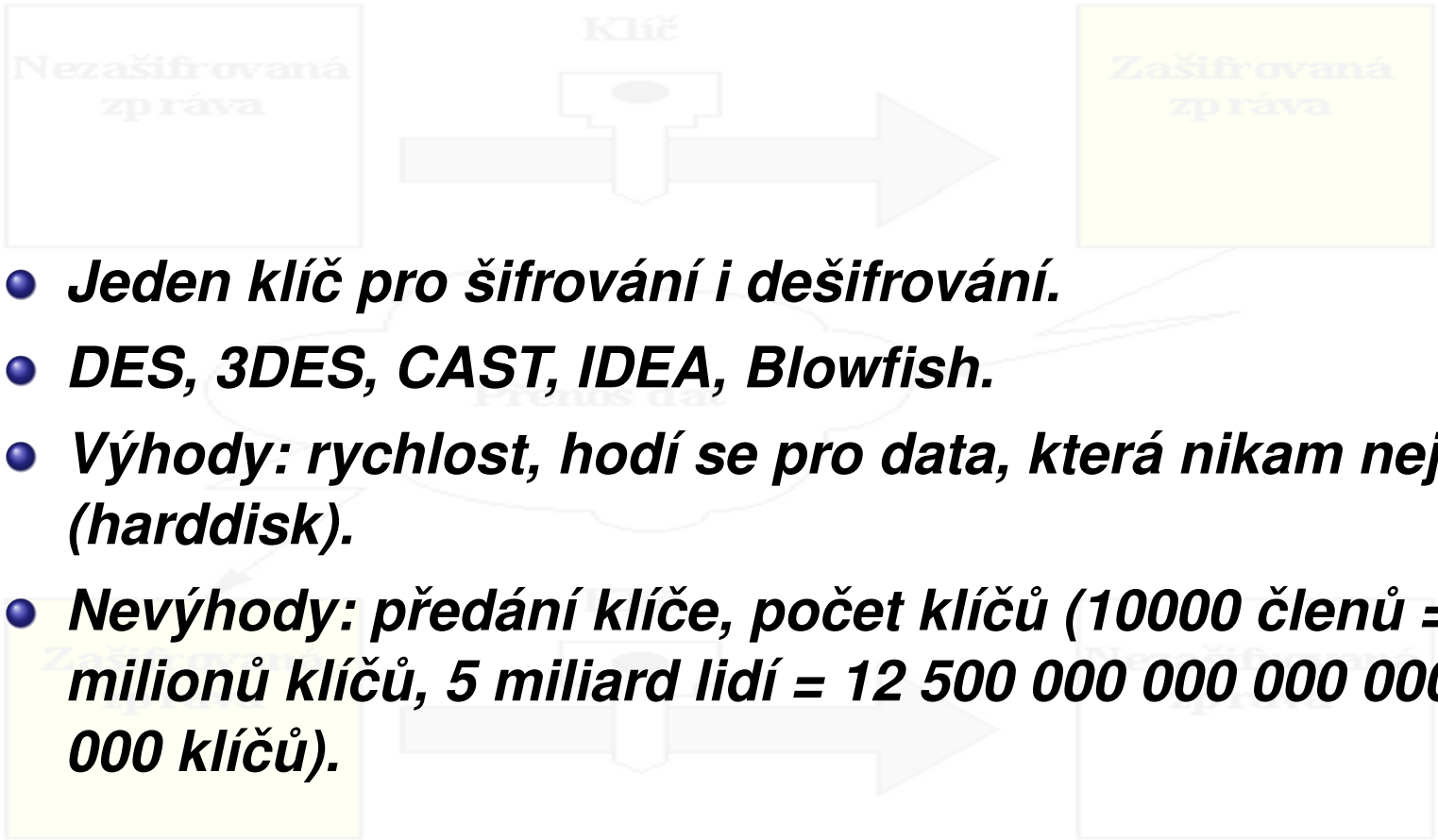
- ***Jeden klíč pro šifrování i dešifrování.***
- ***DES, 3DES, CAST, IDEA, Blowfish.***

Symetrické šifrování



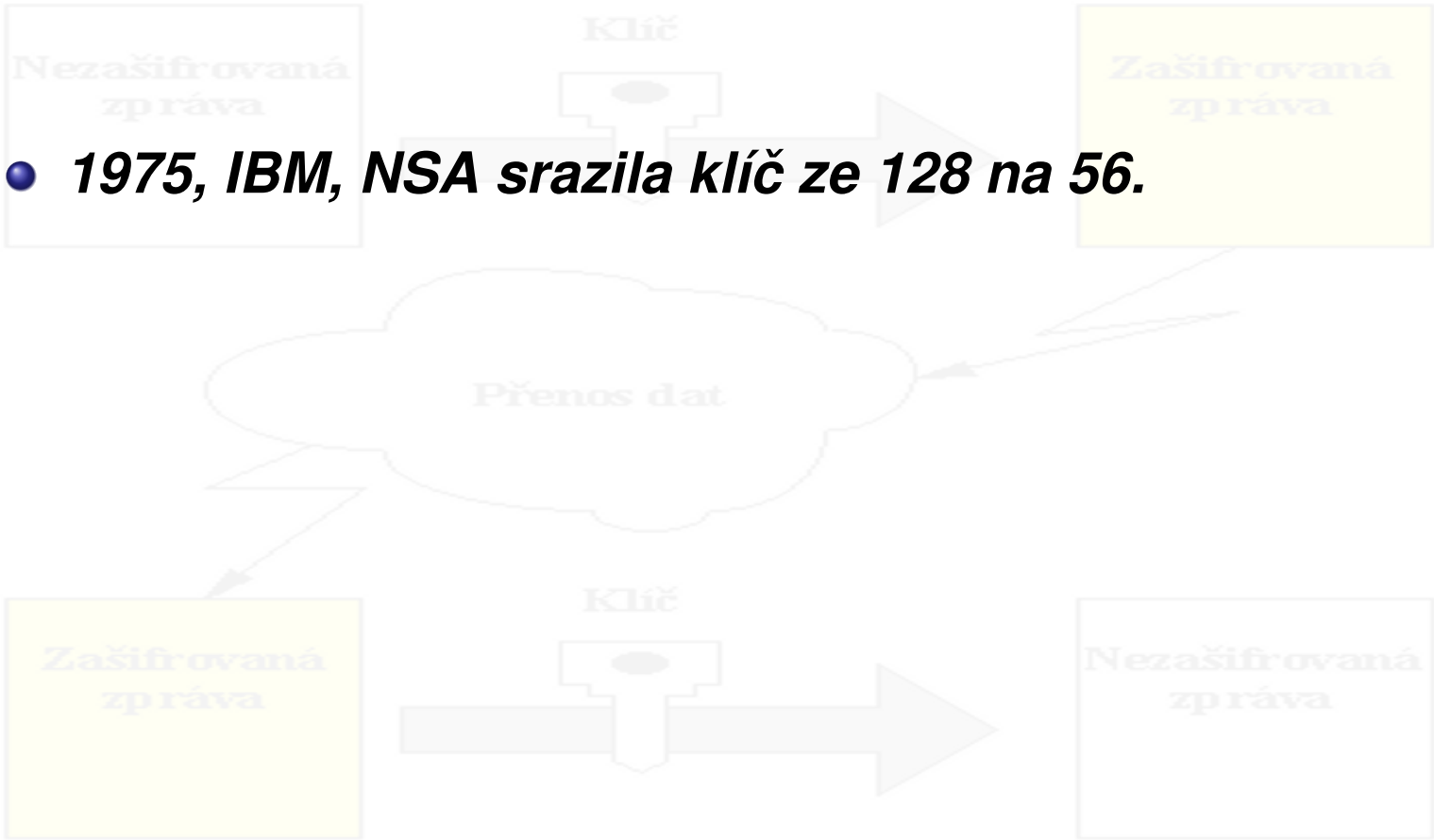
- ***Jeden klíč pro šifrování i dešifrování.***
- ***DES, 3DES, CAST, IDEA, Blowfish.***
- ***Výhody: rychlost, hodí se pro data, která nikam nejdou (harddisk).***

Symetrické šifrování



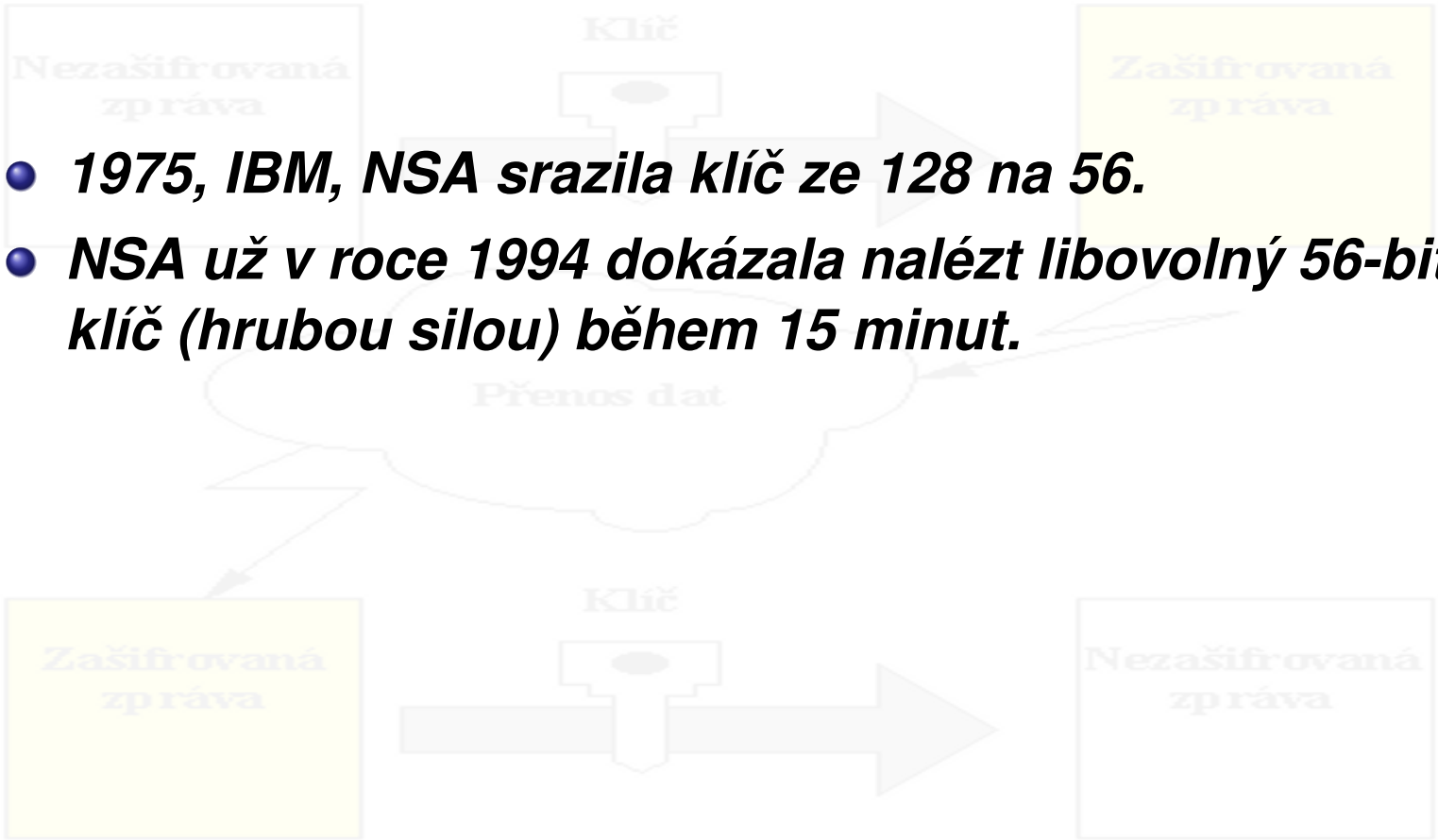
- ***Jeden klíč pro šifrování i dešifrování.***
- ***DES, 3DES, CAST, IDEA, Blowfish.***
- ***Výhody: rychlost, hodí se pro data, která nikam nejdou (harddisk).***
- ***Nevýhody: předání klíče, počet klíčů (10000 členů = 50 milionů klíčů, 5 miliard lidí = 12 500 000 000 000 000 000 klíčů).***

Symetrické šifrování - DES, 3DES



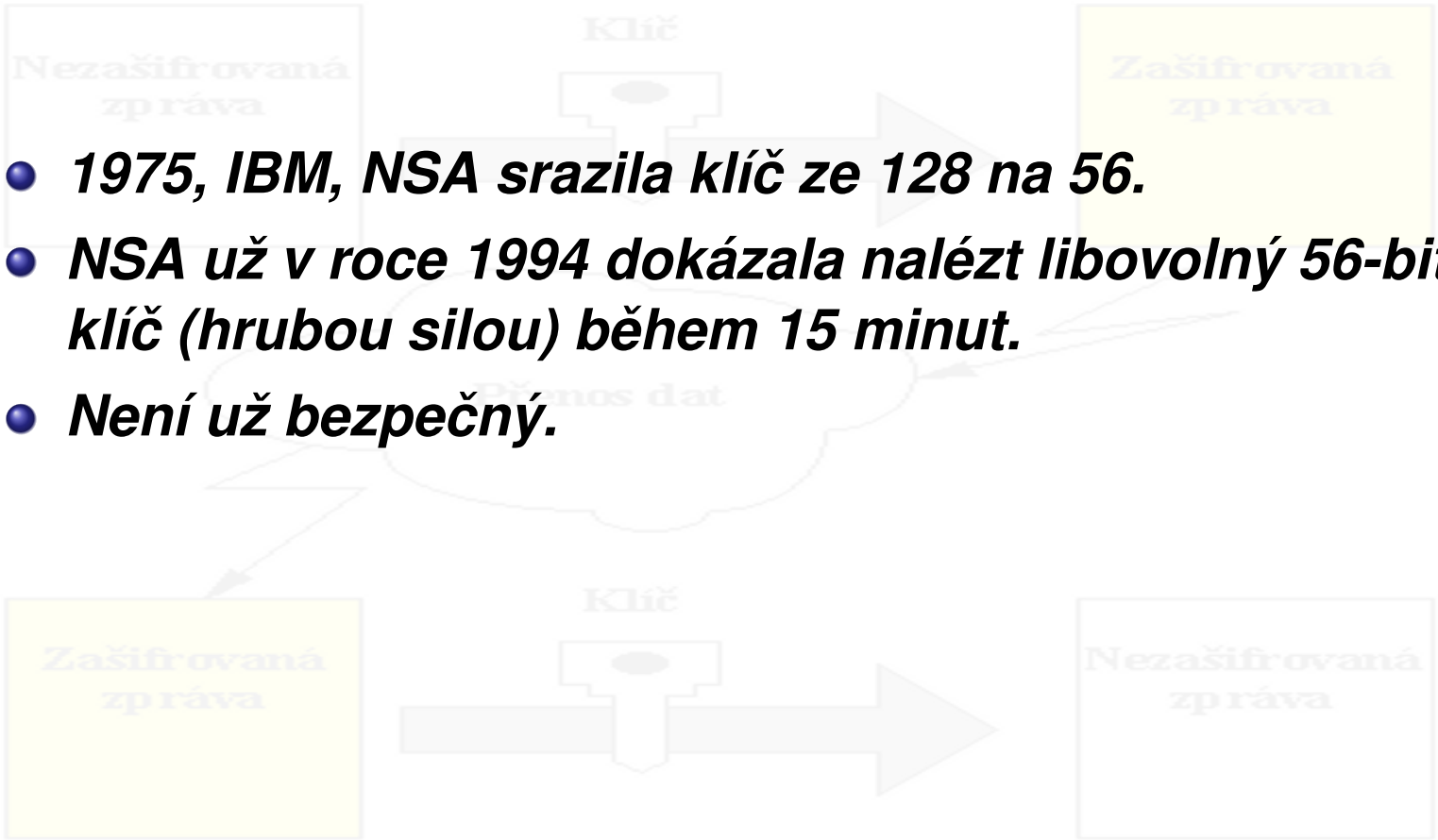
- ***1975, IBM, NSA srazila klíč ze 128 na 56.***

Symetrické šifrování - DES, 3DES



- ***1975, IBM, NSA srazila klíč ze 128 na 56.***
- ***NSA už v roce 1994 dokázala nalézt libovolný 56-bitový klíč (hrubou silou) během 15 minut.***

Symetrické šifrování - DES, 3DES

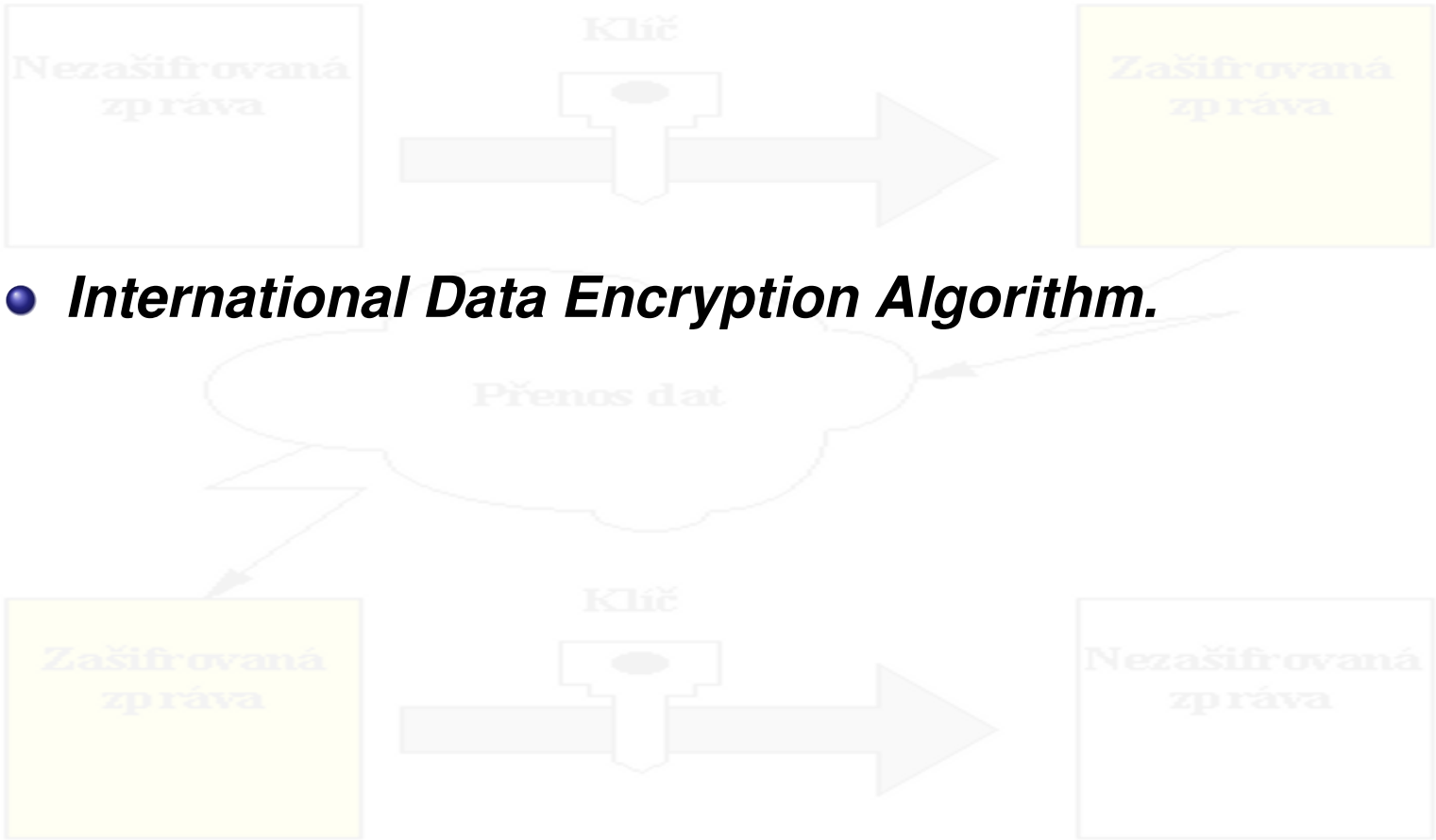


- ***1975, IBM, NSA srazila klíč ze 128 na 56.***
- ***NSA už v roce 1994 dokázala nalézt libovolný 56-bitový klíč (hrubou silou) během 15 minut.***
- ***Není už bezpečný.***

Symetrické šifrování - DES, 3DES

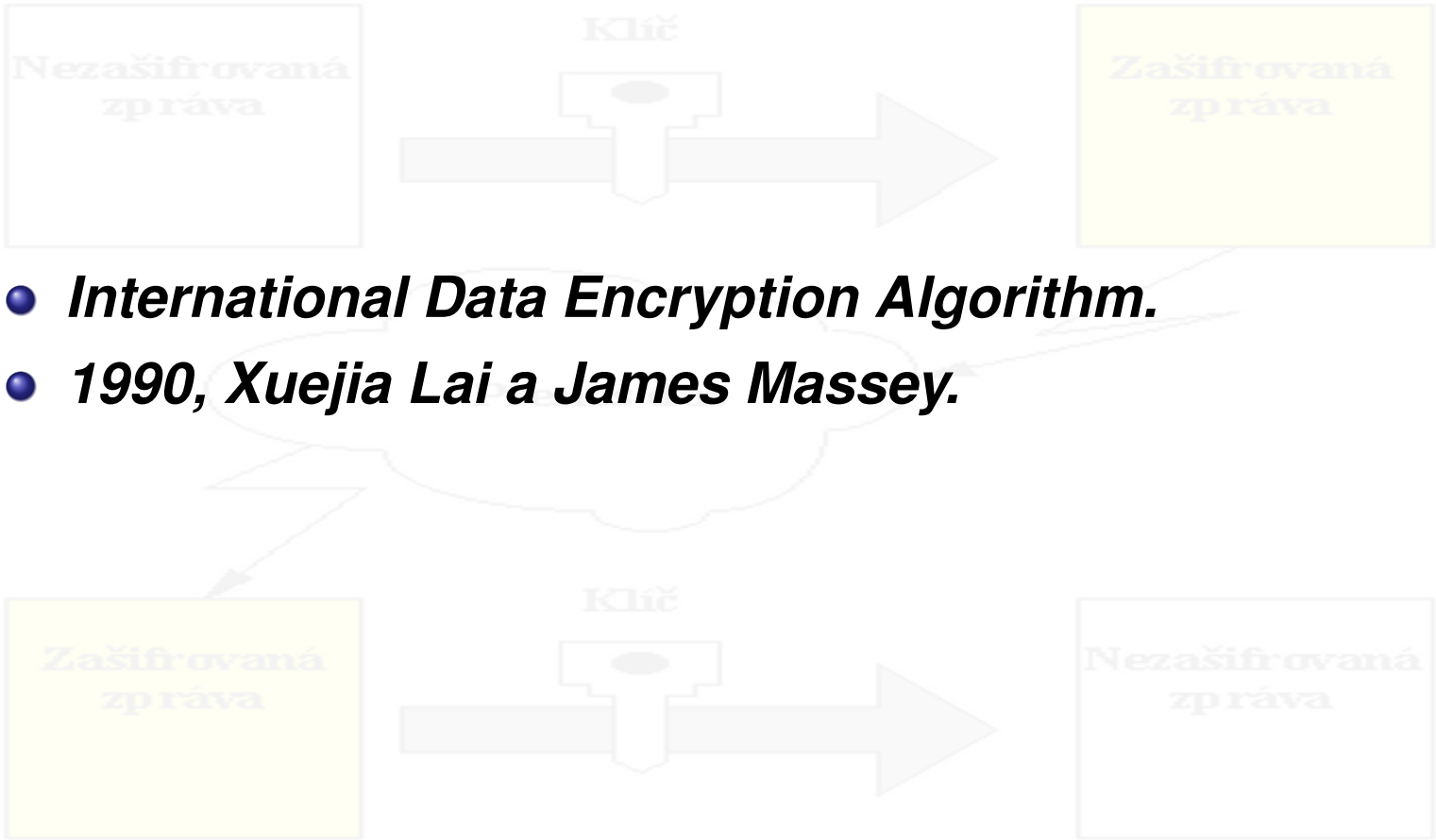
- ***1975, IBM, NSA srazila klíč ze 128 na 56.***
- ***NSA už v roce 1994 dokázala nalézt libovolný 56-bitový klíč (hrubou silou) během 15 minut.***
- ***Není už bezpečný.***
- ***3DES protáhne jedna data algoritmem třikrát - zašifrování nyní probíhá takto: zpráva se zašifruje pomocí algoritmu DES a klíče K_1, odšifruje se pomocí klíče K_2 a opět se zašifruje pomocí klíče K_3 (resp. v jiné verzi klíčem K_1). Délka klíče se tak vlastně 3x (resp. 2x) prodloužila a toto řešení se tímto stalo odolné proti útoku hrubou silou.***

Symetrické šifrování - IDEA



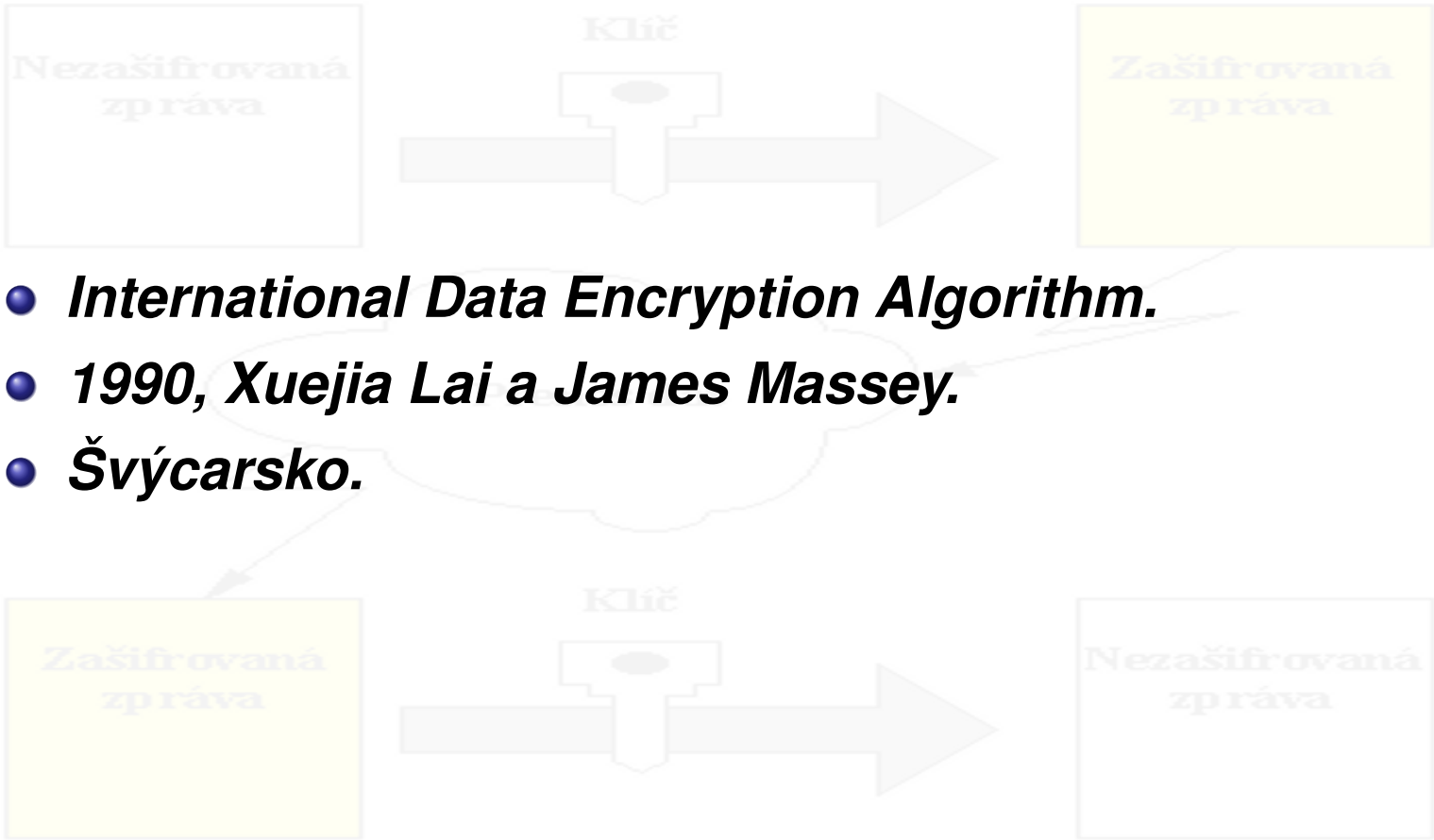
- ***International Data Encryption Algorithm.***

Symetrické šifrování - IDEA



- ***International Data Encryption Algorithm.***
- ***1990, Xuejia Lai a James Massey.***

Symetrické šifrování - IDEA



- ***International Data Encryption Algorithm.***
- ***1990, Xuejia Lai a James Massey.***
- ***Švýcarsko.***

Symetrické šifrování - IDEA

- ***International Data Encryption Algorithm.***
- ***1990, Xuejia Lai a James Massey.***
- ***Švýcarsko.***
- ***Klíč 128 bitů.***

Symetrické šifrování - IDEA

- ***International Data Encryption Algorithm.***
- ***1990, Xuejia Lai a James Massey.***
- ***Švýcarsko.***
- ***Klíč 128 bitů.***
- ***Implementována v rámci SSL.***

Symetrické šifrování - IDEA

- ***International Data Encryption Algorithm.***
- ***1990, Xuejia Lai a James Massey.***
- ***Švýcarsko.***
- ***Klíč 128 bitů.***
- ***Implementována v rámci SSL.***
- ***Není známo, že by byla rozluštěna metodou hrubé síly.***

Symetrické šifrování - AES

- V roce 1997 NIST vypisuje veřejnou soutěž na vytvoření nového komerčního standardu pro symetrické šifrování.

Symetrické šifrování - AES

- V roce 1997 NIST vypisuje veřejnou soutěž na vytvoření nového komerčního standardu pro symetrické šifrování.
- Novým standardem se stal ***AES***, dříve zvaný Rijndael, (***Advanced Encryption Standard***).

Symetrické šifrování - AES

- V roce 1997 NIST vypisuje veřejnou soutěž na vytvoření nového komerčního standardu pro symetrické šifrování.
- Novým standardem se stal ***AES***, dříve zvaný Rijndael, (***Advanced Encryption Standard***).
- Je to nejpoužívanější algoritmus pro šifrování důležitých údajů. Používají ho různé organizace, od Applu a Microsoftu po NSA.

Symetrické šifrování - AES

- V roce 1997 NIST vypisuje veřejnou soutěž na vytvoření nového komerčního standardu pro symetrické šifrování.
- Novým standardem se stal ***AES***, dříve zvaný Rijndael, (***Advanced Encryption Standard***).
- Je to nejpoužívanější algoritmus pro šifrování důležitých údajů. Používají ho různé organizace, od Applu a Microsoftu po NSA.
- Celkově existují 3 blokové šifry, ze kterých se AES skládá, a to 128bitové, 192bitové a 256bitové.Každá z AES šifer šifruje a dešifruje data v blocích po 128 bitech pomocí kryptografického klíče ze 128, 192 a 256 bitů – 256bitový je nejbezpečnější.

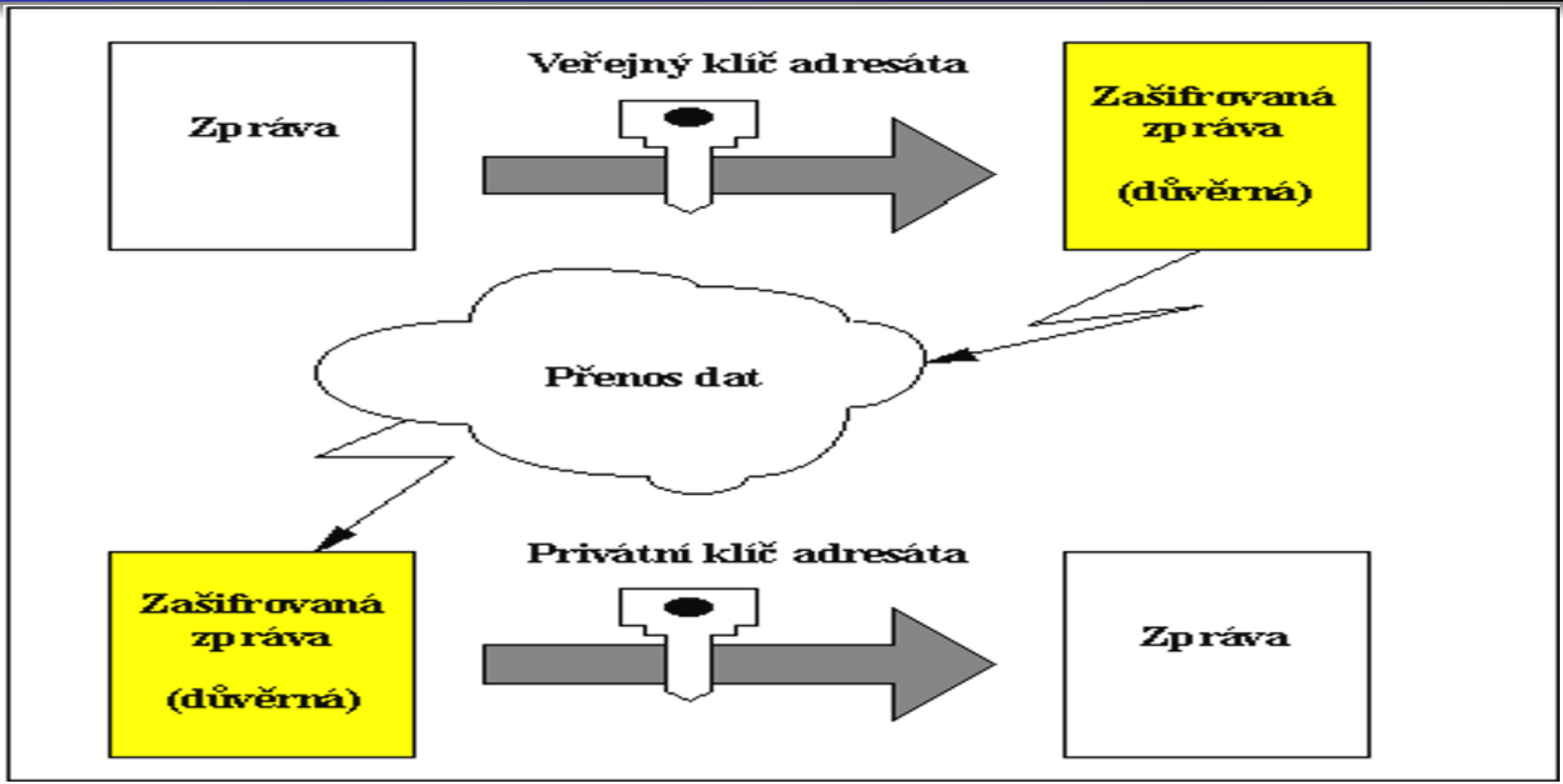
Symetrické šifrování - AES

- V roce 1997 NIST vypisuje veřejnou soutěž na vytvoření nového komerčního standardu pro symetrické šifrování.
- Novým standardem se stal ***AES***, dříve zvaný Rijndael, (***Advanced Encryption Standard***).
- Je to nejpoužívanější algoritmus pro šifrování důležitých údajů. Používají ho různé organizace, od Applu a Microsoftu po NSA.
- Celkově existují 3 blokové šifry, ze kterých se AES skládá, a to 128bitové, 192bitové a 256bitové.Každá z AES šifer šifruje a dešifruje data v blocích po 128 bitech pomocí kryptografického klíče ze 128, 192 a 256 bitů – 256bitový je nejbezpečnější.
- Je určen pro všechny typy aplikací a nasazení.

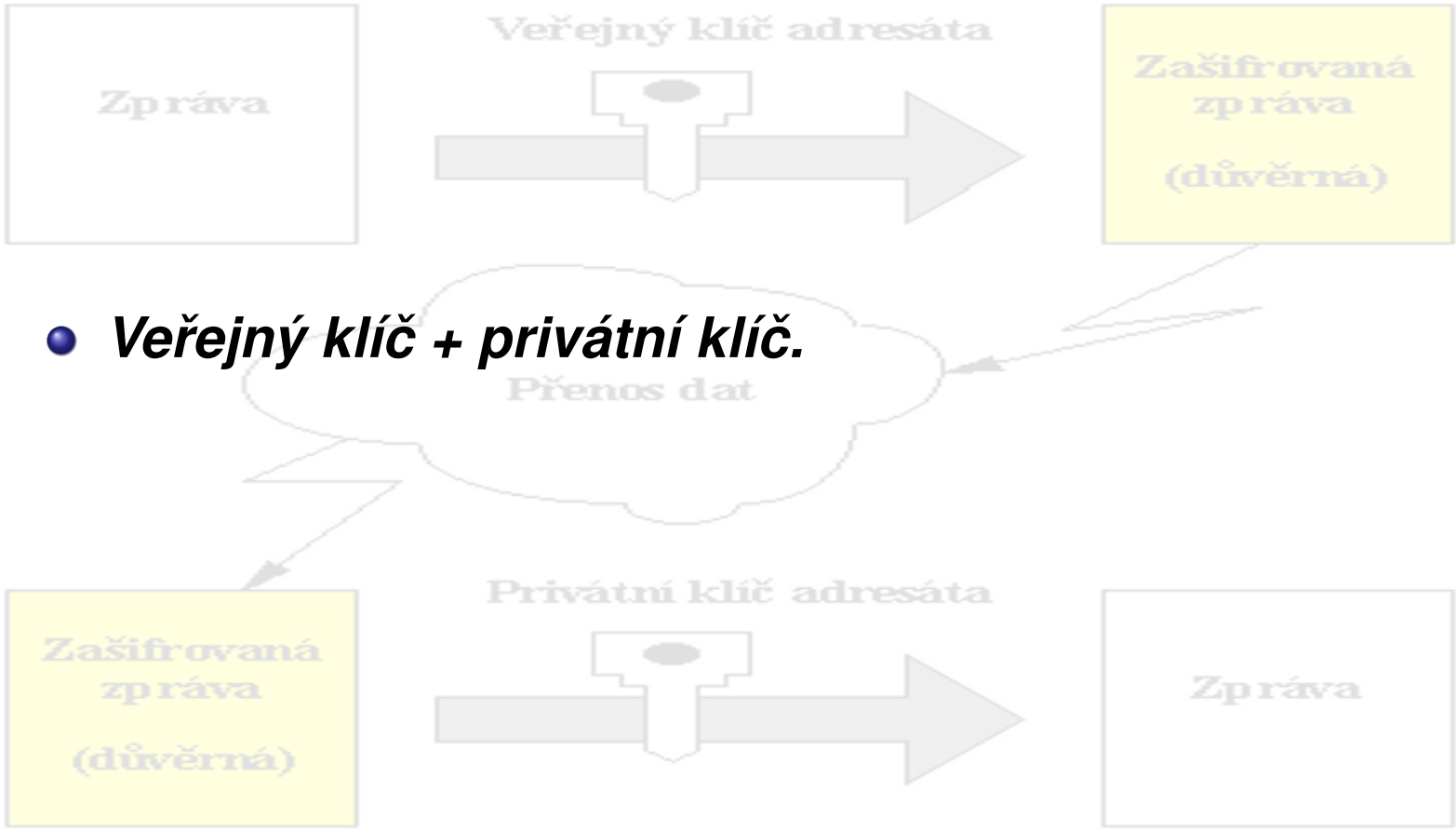
Symetrické šifrování - AES

- V roce 1997 NIST vypisuje veřejnou soutěž na vytvoření nového komerčního standardu pro symetrické šifrování.
- Novým standardem se stal ***AES***, dříve zvaný Rijndael, (***Advanced Encryption Standard***).
- Je to nejpoužívanější algoritmus pro šifrování důležitých údajů. Používají ho různé organizace, od Applu a Microsoftu po NSA.
- Celkově existují 3 blokové šifry, ze kterých se AES skládá, a to 128bitové, 192bitové a 256bitové.Každá z AES šifer šifruje a dešifruje data v blocích po 128 bitech pomocí kryptografického klíče ze 128, 192 a 256 bitů – 256bitový je nejbezpečnější.
- Je určen pro všechny typy aplikací a nasazení.
- Algoritmus není patentován a vítěz dostává odměnu "***zlatý vavřín kryptologie".***

Asymetrické šifrování

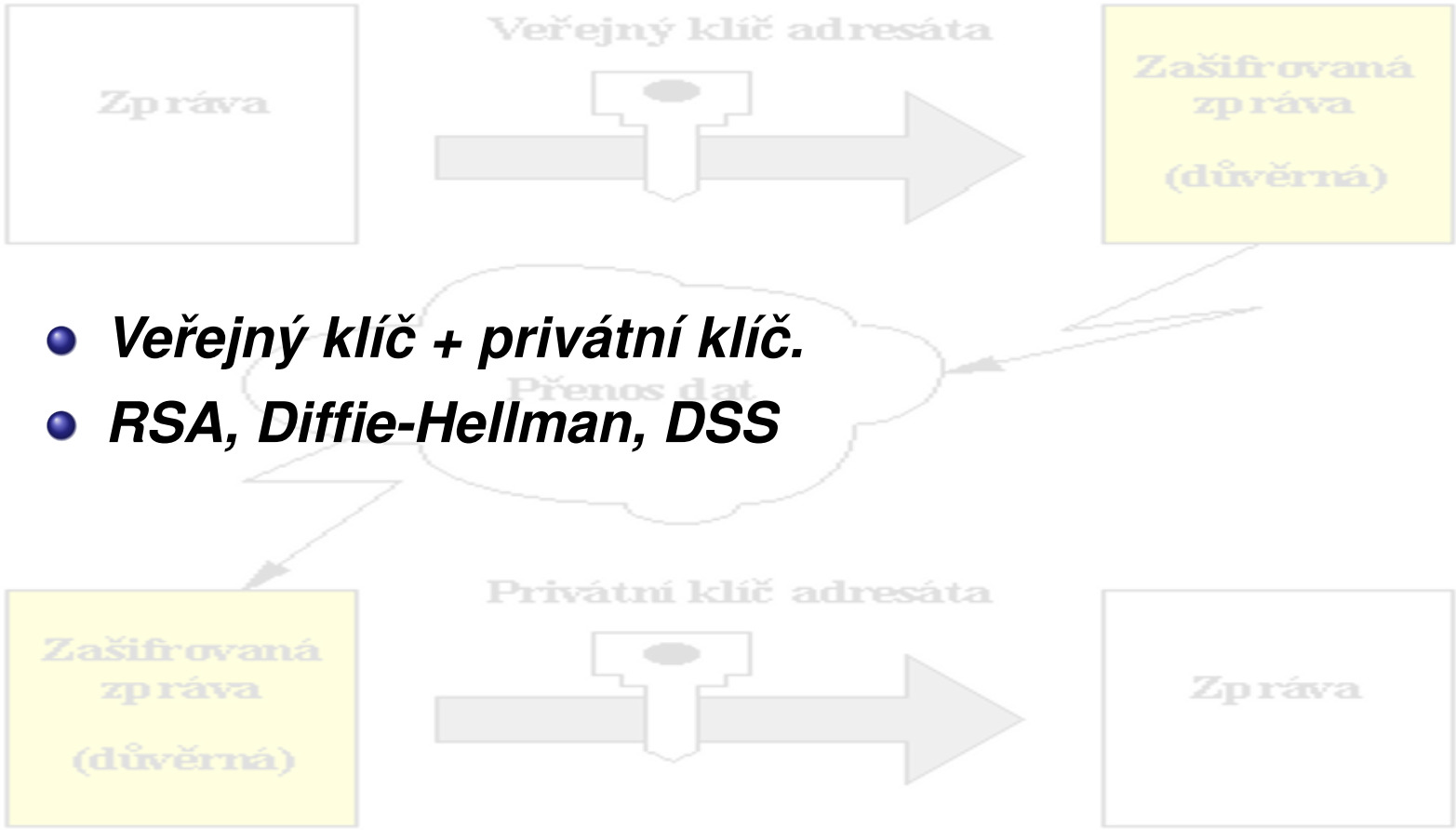


Asymetrické šifrování



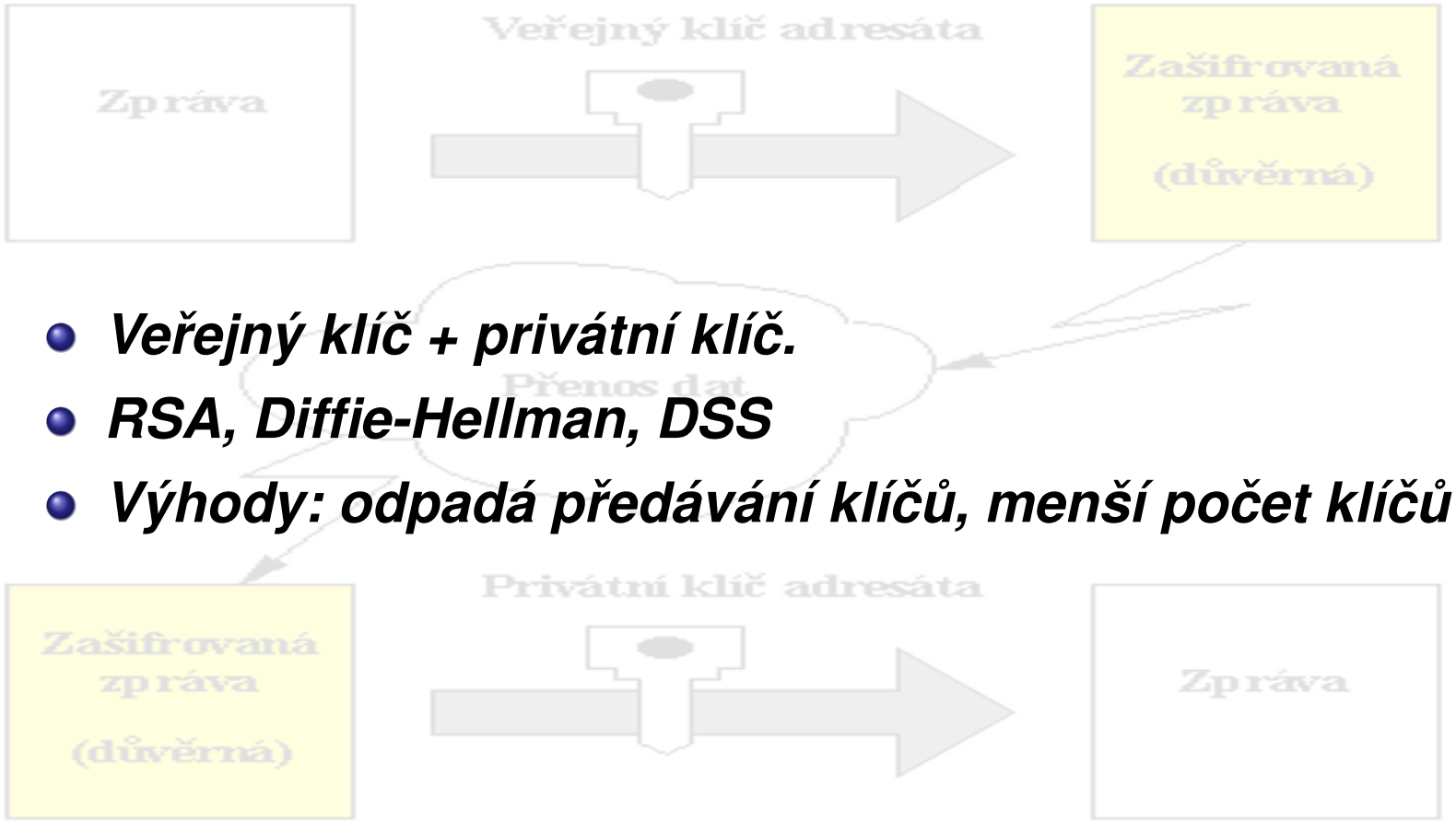
- ***Veřejný klíč + privátní klíč.***

Asymetrické šifrování



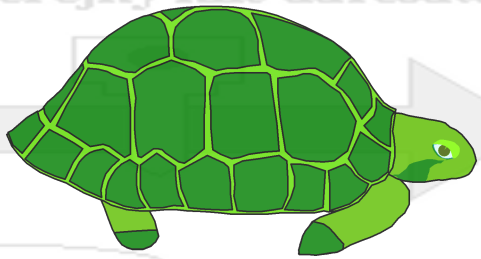
- ***Veřejný klíč + privátní klíč.***
- ***RSA, Diffie-Hellman, DSS***

Asymetrické šifrování

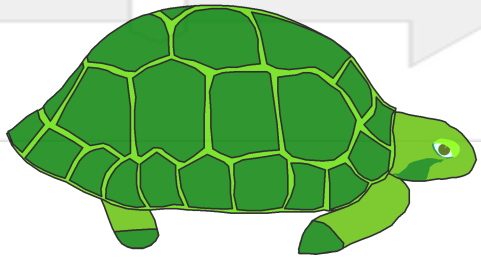


- ***Veřejný klíč + privátní klíč.***
- ***RSA, Diffie-Hellman, DSS***
- ***Výhody: odpadá předávání klíčů, menší počet klíčů***

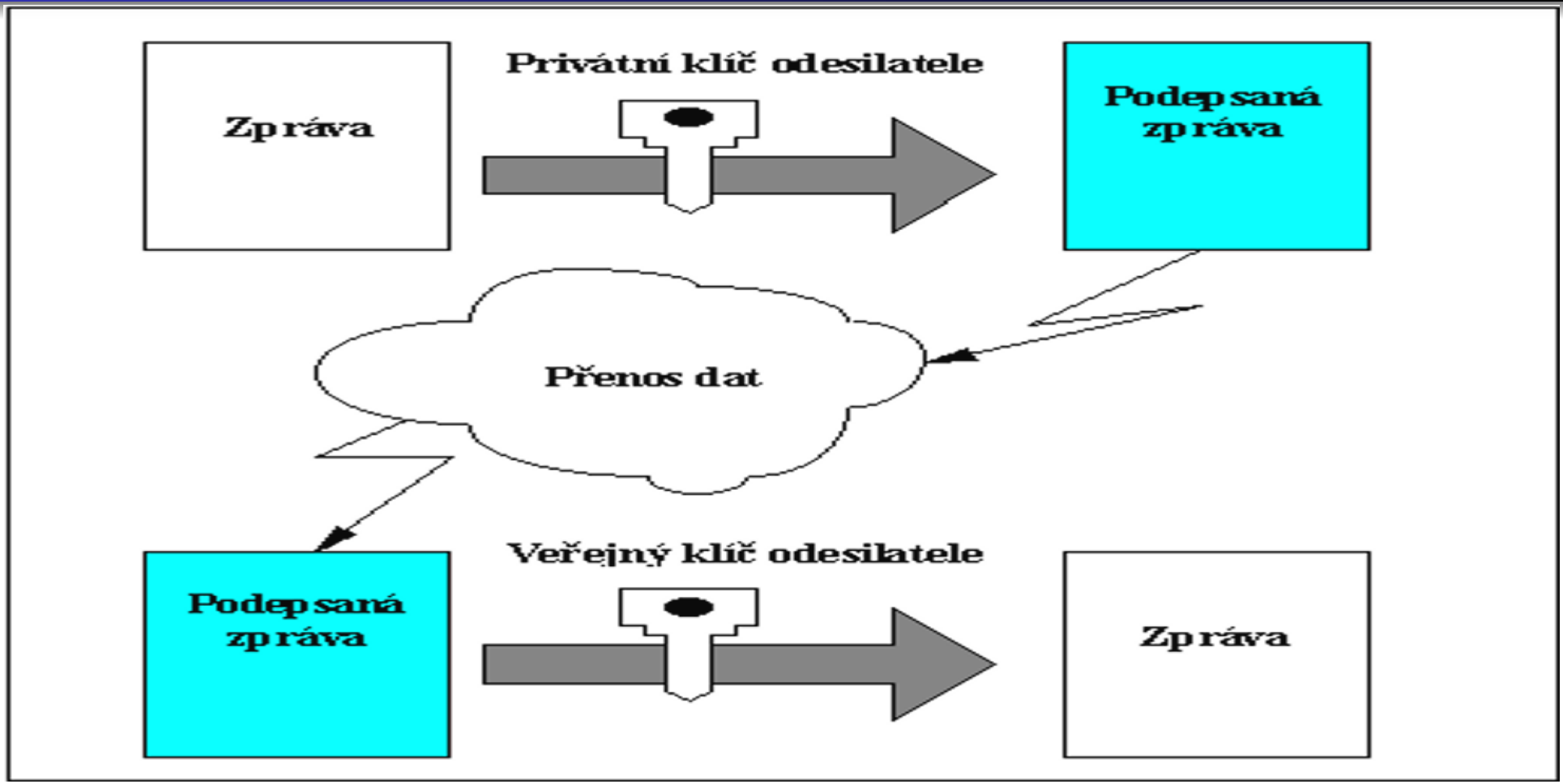
Asymetrické šifrování



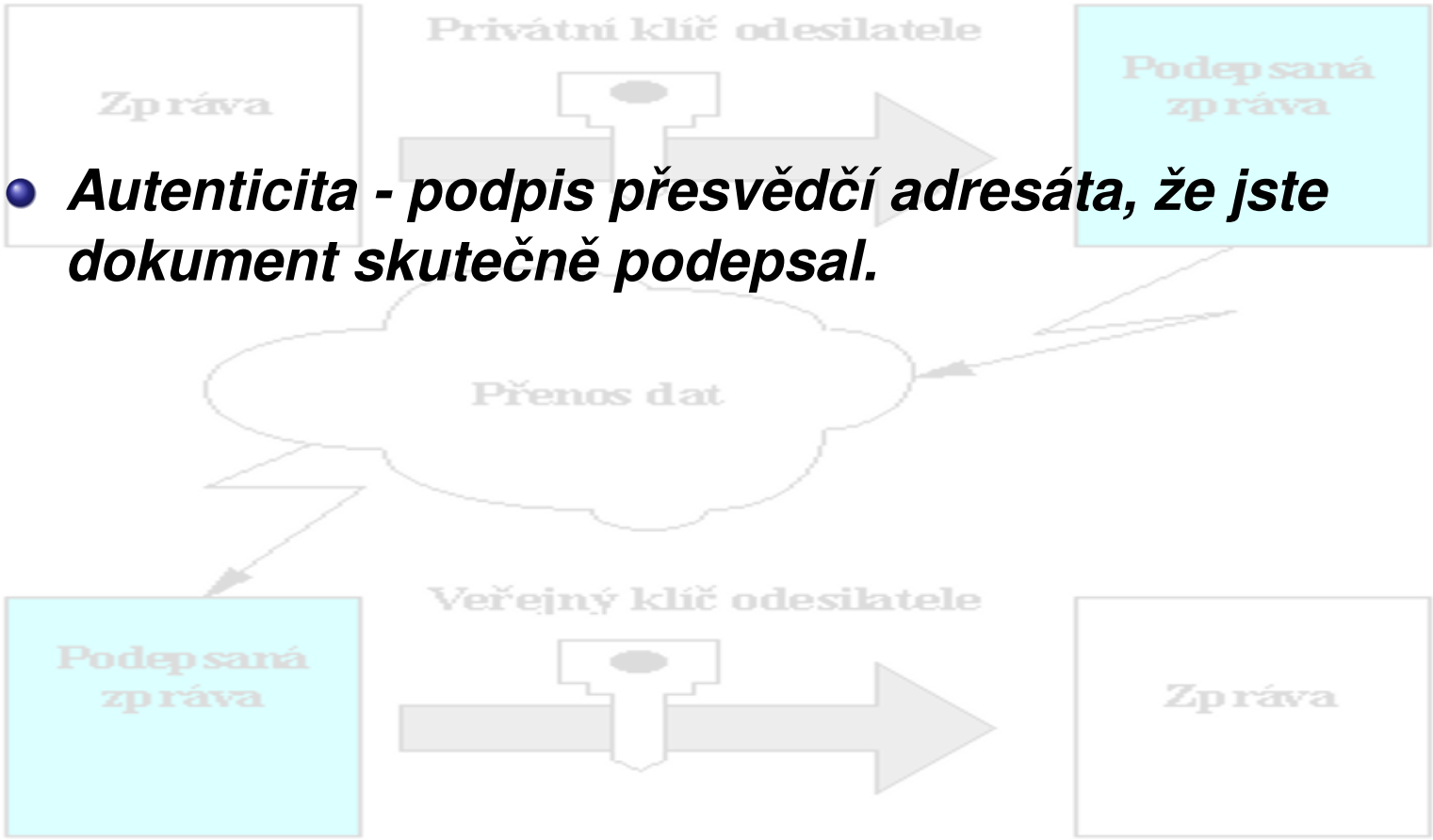
- ***Veřejný klíč + privátní klíč.***
- ***RSA, Diffie-Hellman, DSS***
- ***Výhody: odpadá předávání klíčů, menší počet klíčů***
- ***Nevýhody: „pomalost“ (asi 1000x pomalejší)***



Digitální podpis

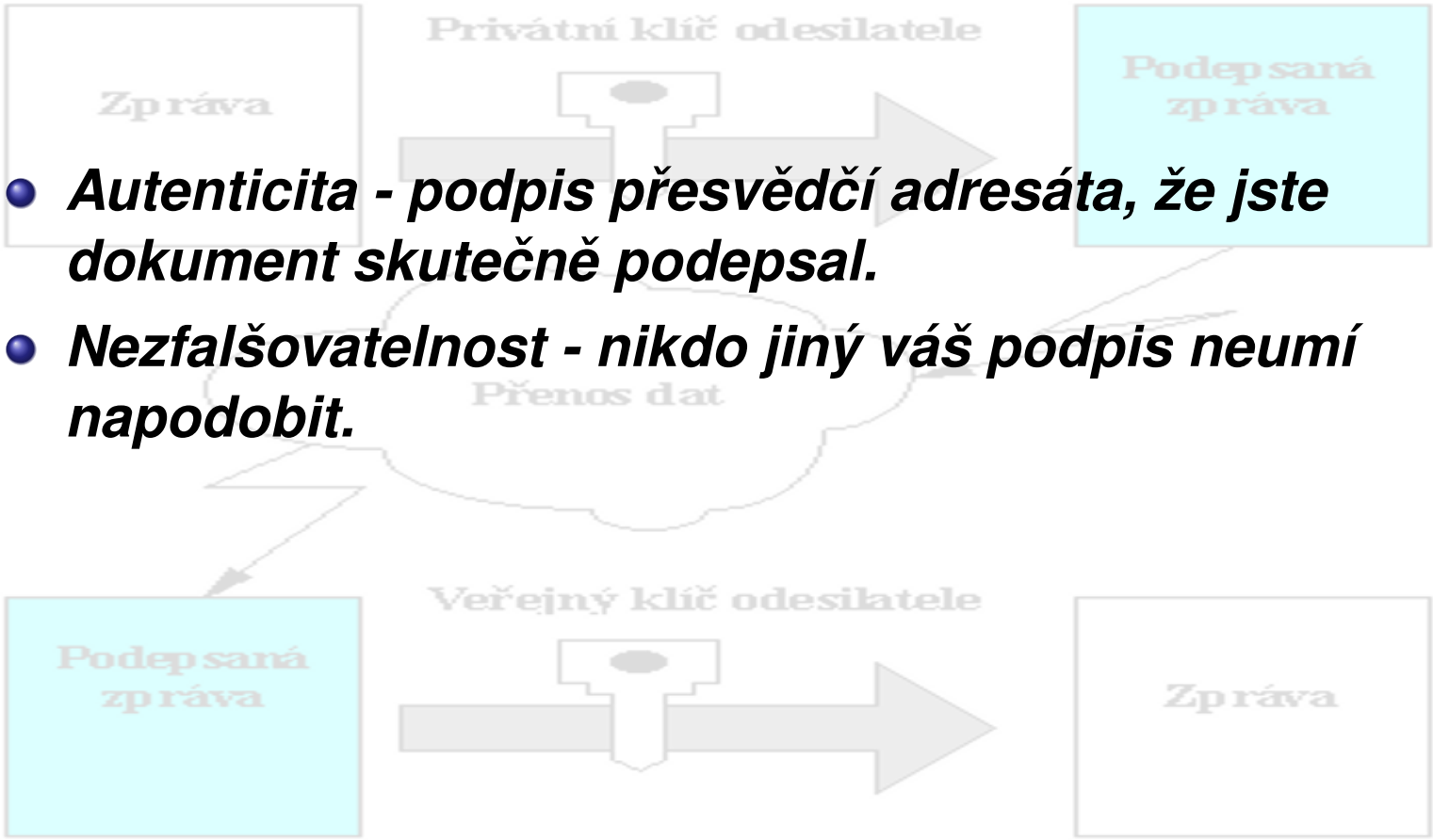


Digitální podpis



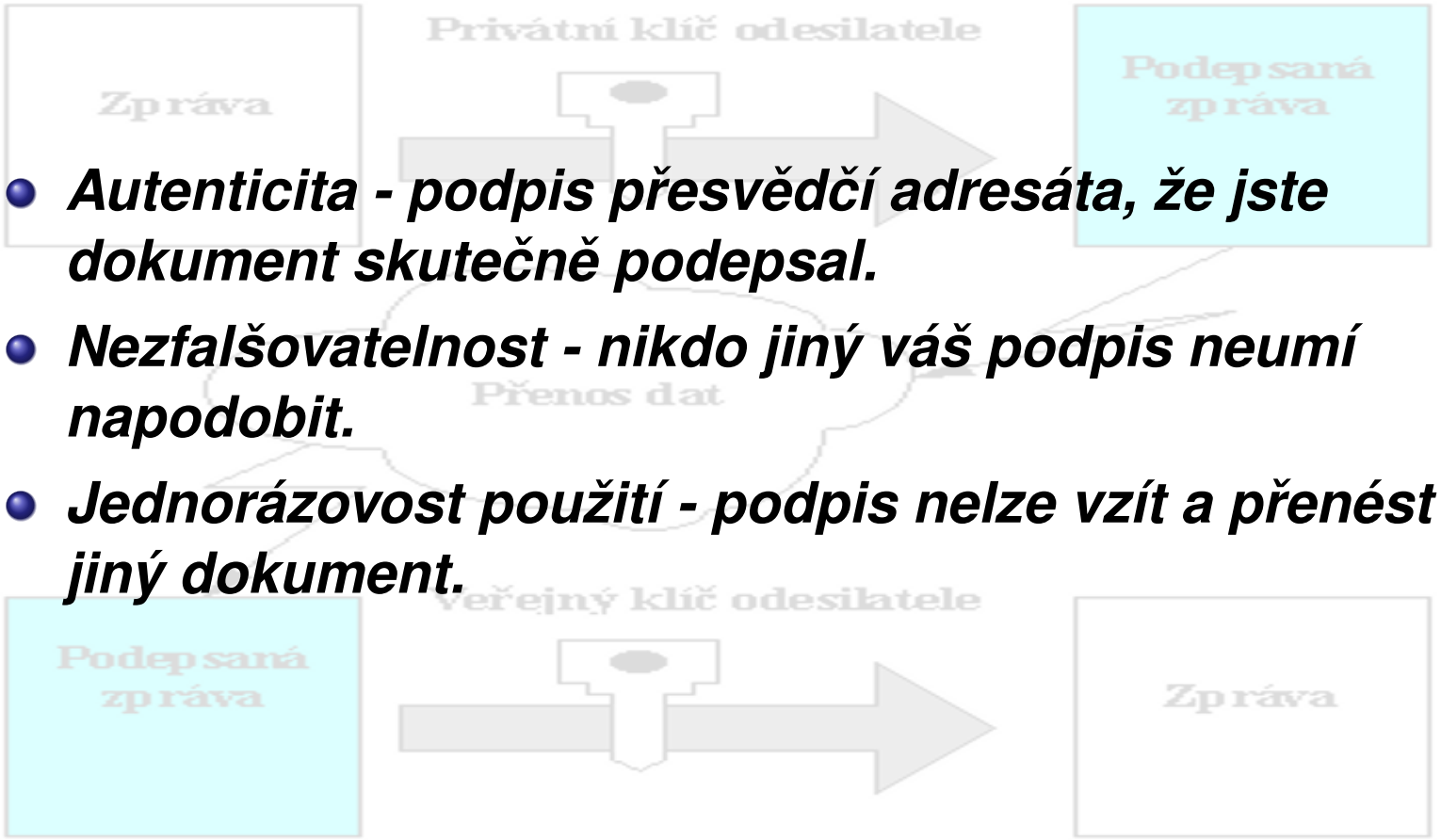
- ***Autenticita - podpis přesvědčí adresáta, že jste dokument skutečně podepsal.***

Digitální podpis



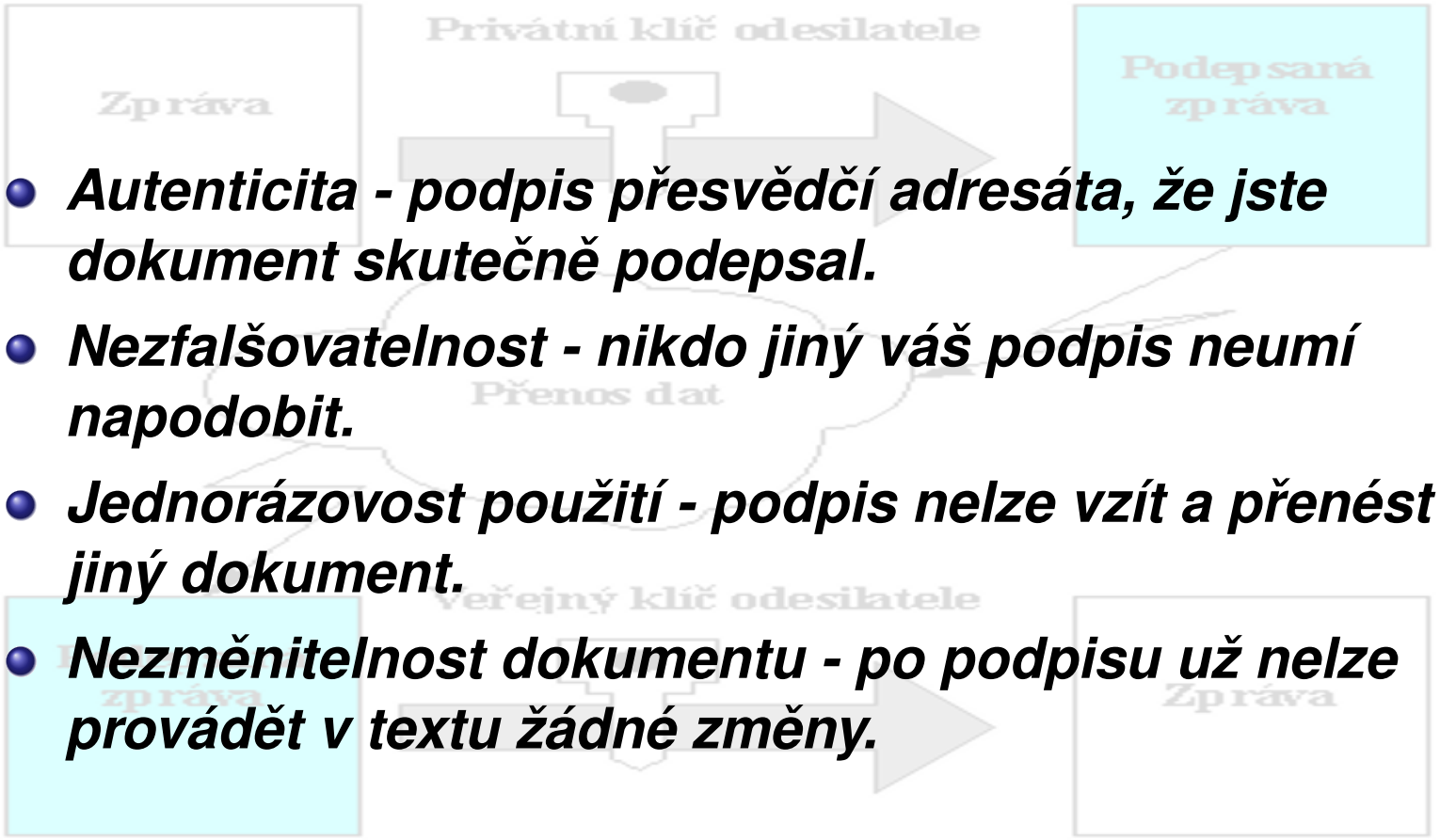
- ***Autenticita - podpis přesvědčí adresáta, že jste dokument skutečně podepsal.***
- ***Nezfalšovatelnost - nikdo jiný váš podpis neumí napodobit.***

Digitální podpis



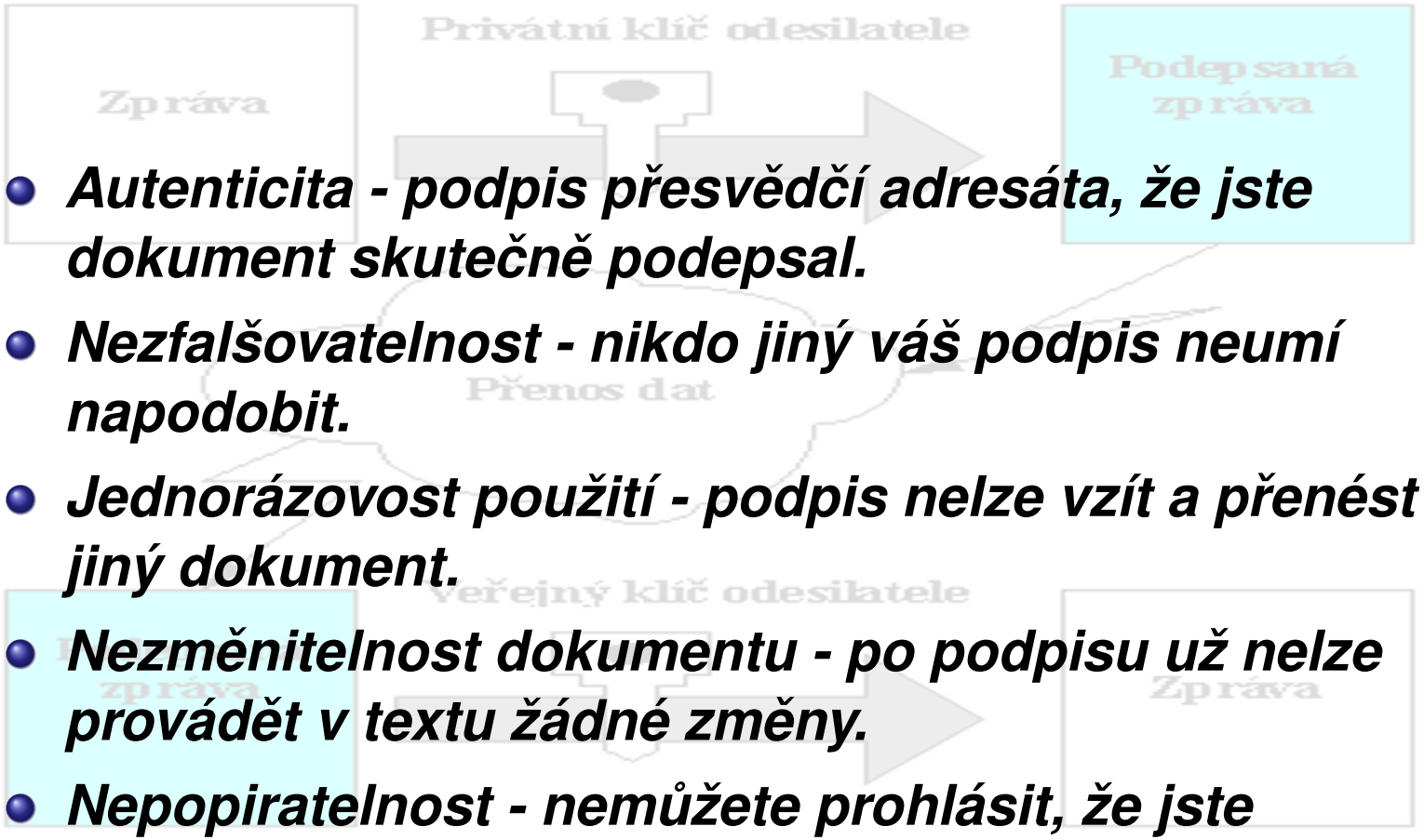
- ***Autenticita - podpis přesvědčí adresáta, že jste dokument skutečně podepsal.***
- ***Nezfalšovatelnost - nikdo jiný váš podpis neumí napodobit.***
- ***Jednorázovost použití - podpis nelze vzít a přenést na jiný dokument.***

Digitální podpis



- ***Autenticita - podpis přesvědčí adresáta, že jste dokument skutečně podepsal.***
- ***Nezfalšovatelnost - nikdo jiný váš podpis neumí napodobit.***
- ***Jednorázovost použití - podpis nelze vzít a přenést na jiný dokument.***
- ***Nezměnitelnost dokumentu - po podpisu už nelze provádět v textu žádné změny.***

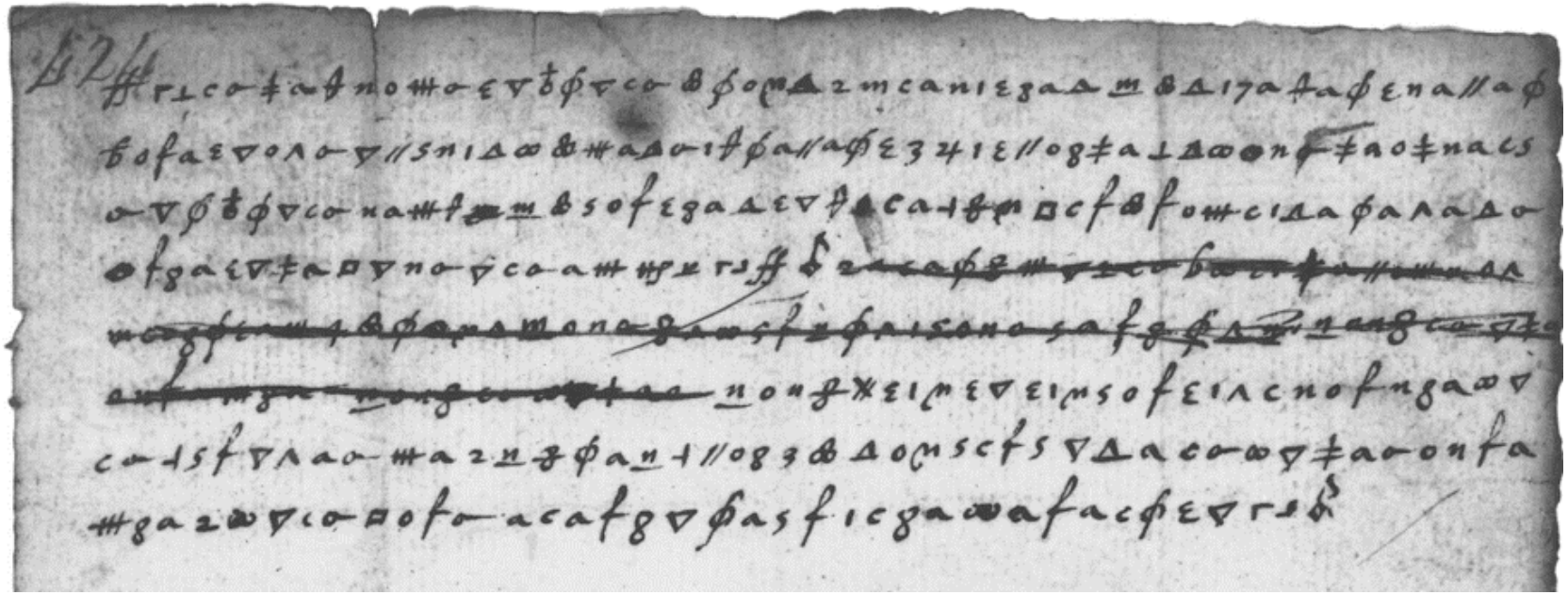
Digitální podpis



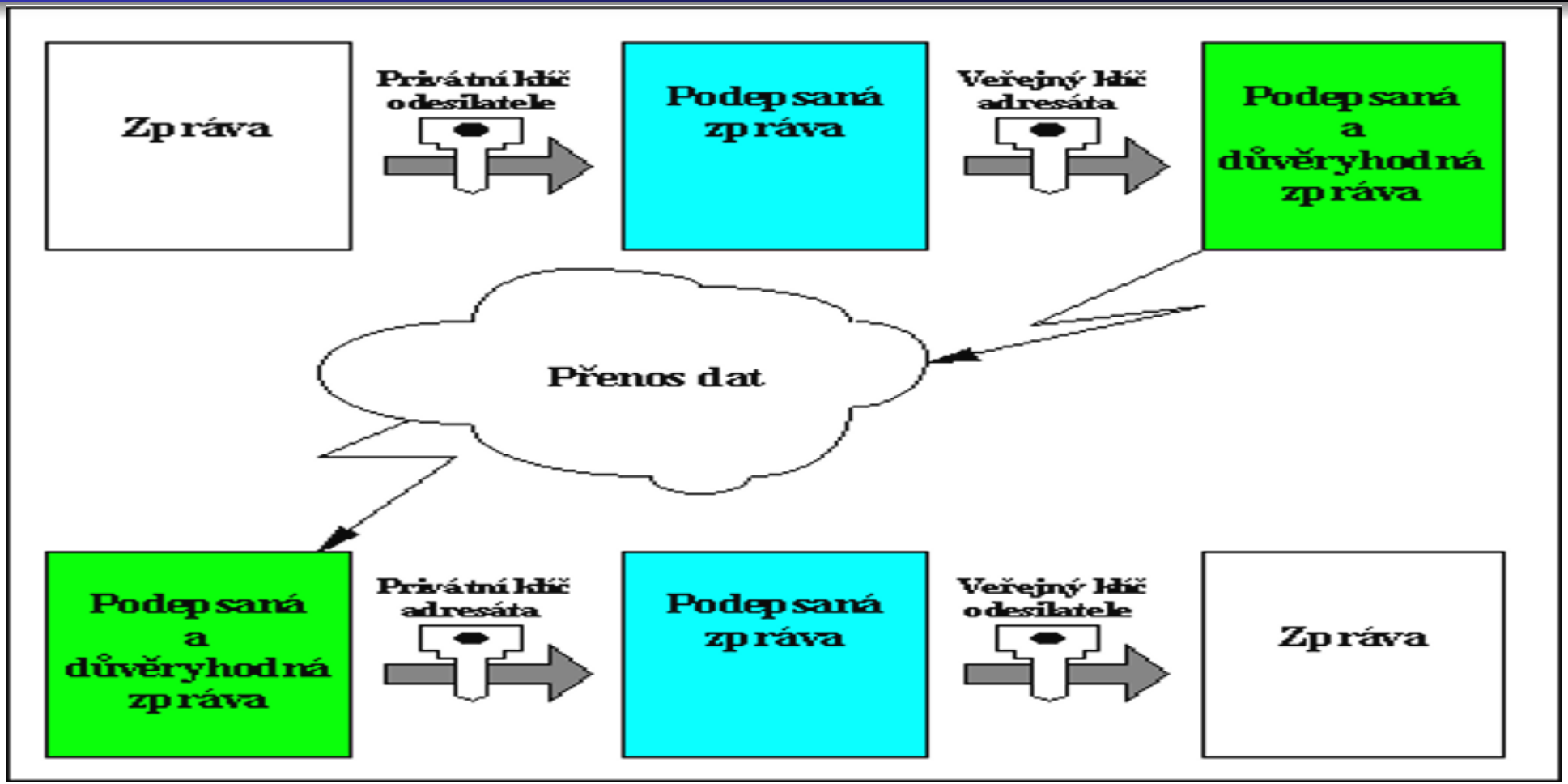
- ***Autenticita - podpis přesvědčí adresáta, že jste dokument skutečně podepsal.***
- ***Nezfalšovatelnost - nikdo jiný váš podpis neumí napodobit.***
- ***Jednorázovost použití - podpis nelze vzít a přenést na jiný dokument.***
- ***Nezměnitelnost dokumentu - po podpisu už nelze provádět v textu žádné změny.***
- ***Nepopiratelnost - nemůžete prohlásit, že jste dokument nepodepsal, když je vámi podepsaný.***

Digitální podpis

Na obrázku vidíme zachycený šifrovaný dopis Marie Stuartovny. Luštitel, který ***znal šifrovací klíč***, vložil závěrečnou část zprávy, žádající sdělení jmen a adres spiklenců, spolupracujících s Marií Stuartovnou. Na základě toho byli spiklenci odhaleni.



Digitální podpis



Hašovací funkce

- Hašovací funkce umí vytvořit z jakkoliv velkých dat jejich identifikátor - digitální otisk dat.

Hašovací funkce

- Hašovací funkce umí vytvořit z jakkoliv velkých dat jejich identifikátor - digitální otisk dat.
- Data lze nyní identifikovat (a to i z právního hlediska) podle jejich digitálního otisku majícího řádově pár set bitů.

Hašovací funkce

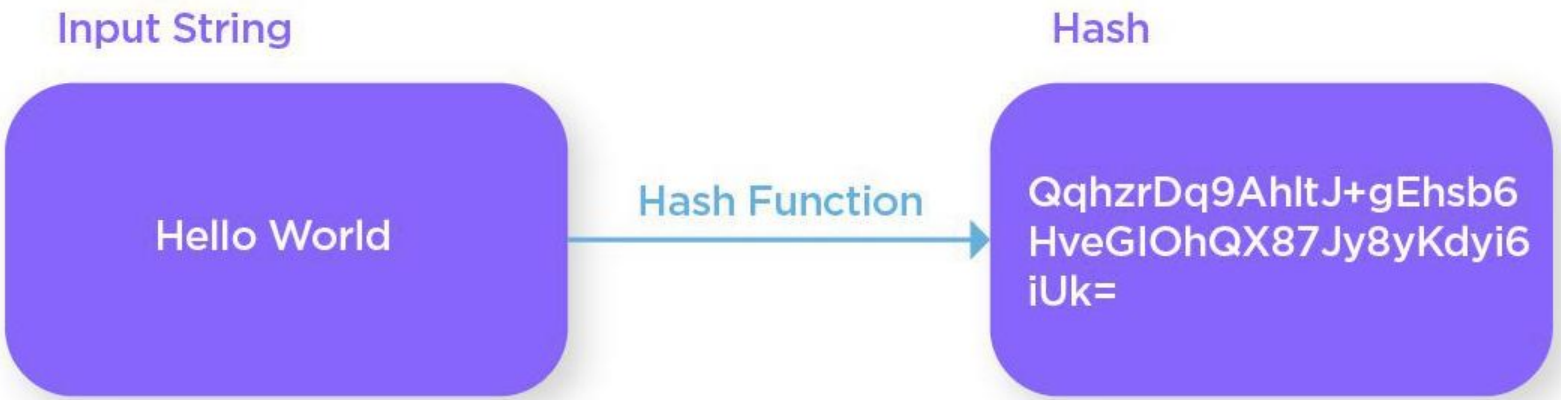
- Hašovací funkce umí vytvořit z jakkoliv velkých dat jejich identifikátor - digitální otisk dat.
- Data lze nyní identifikovat (a to i z právního hlediska) podle jejich digitálního otisku majícího řádově pár set bitů.
- Příklady:
  a) Kontrola shody databází, otisky dat.

Hašovací funkce

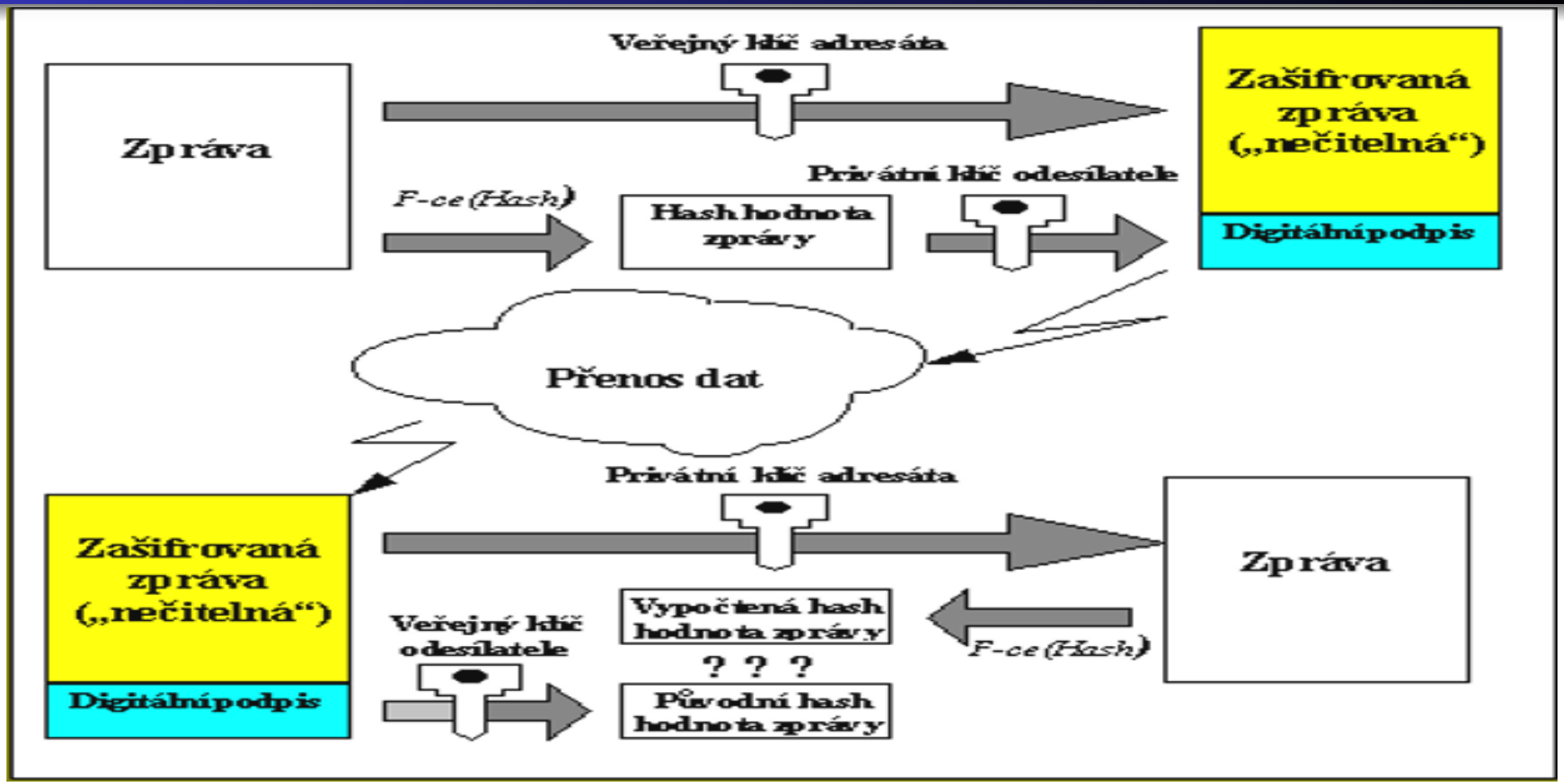
- Hašovací funkce umí vytvořit z jakkoliv velkých dat jejich identifikátor - digitální otisk dat.
- Data lze nyní identifikovat (a to i z právního hlediska) podle jejich digitálního otisku majícího řádově pár set bitů.
- Příklady:
  a) Kontrola shody databází, otisky dat.
  b) Prokazování autorství.

Hašovací funkce

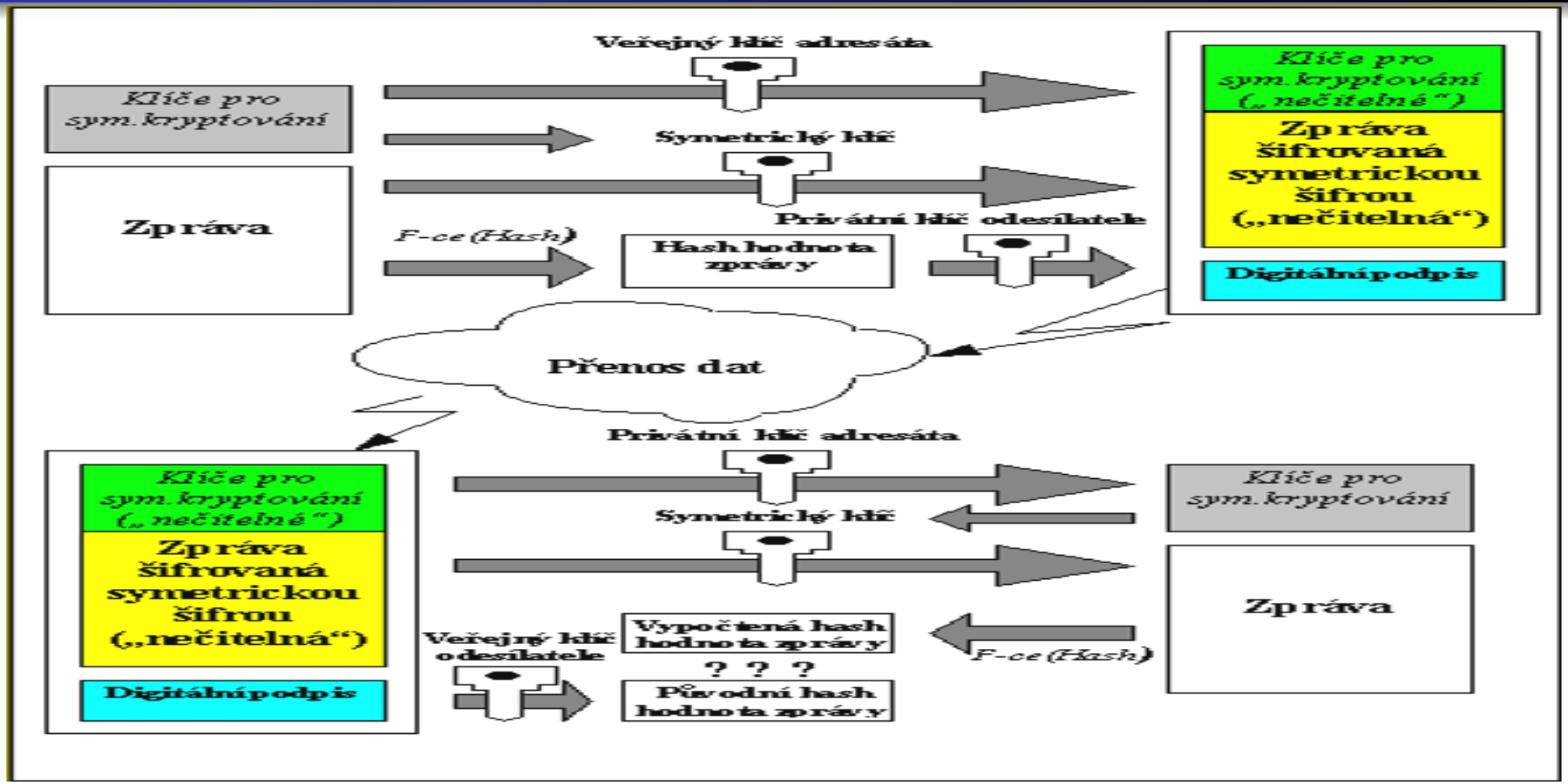
- Hašovací funkce umí vytvořit z jakkoliv velkých dat jejich identifikátor - digitální otisk dat.
- Data lze nyní identifikovat (a to i z právního hlediska) podle jejich digitálního otisku majícího řádově pár set bitů.
- Příklady:
  a) Kontrola shody databází, otisky dat.
  b) Prokazování autorství.
  c) Ukládání přihlašovacích hesel.



Hašovací funkce a digitální podpis



Hašovací funkce a digitální podpis ještě jednou



RSA

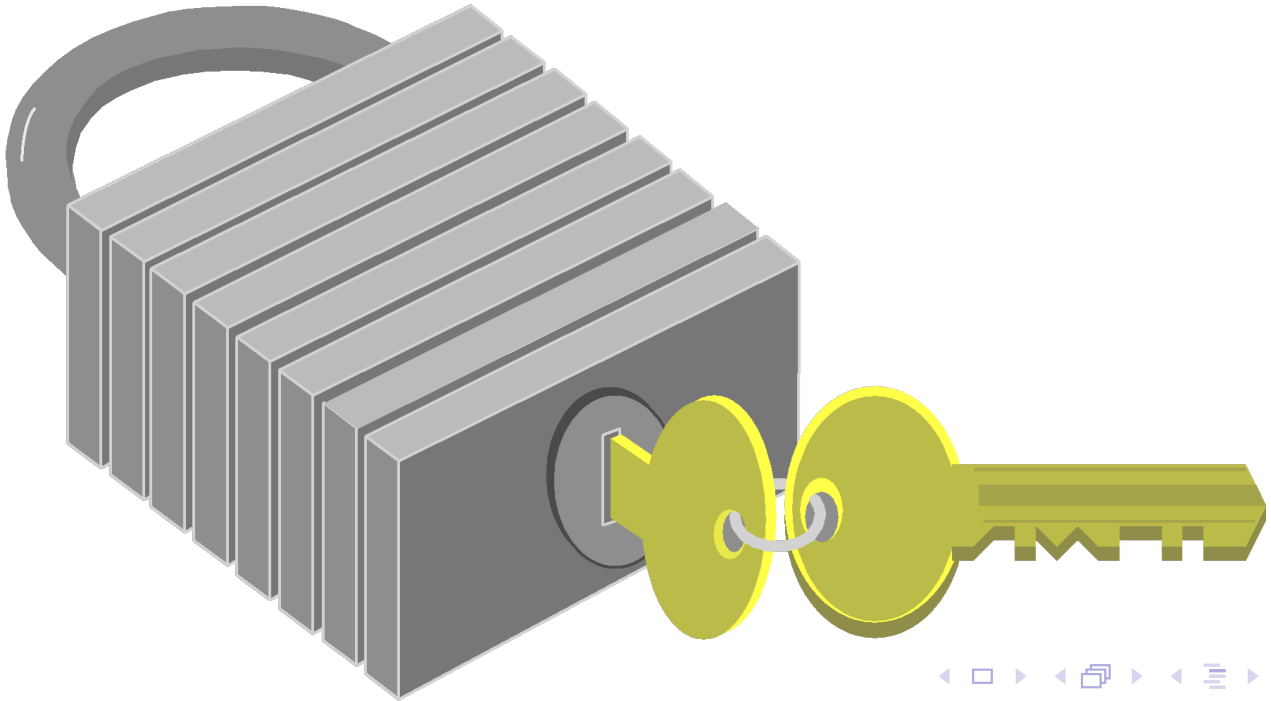
- ***Ron Rivest, Adi Shamir a Len Adleman (1977).***

RSA

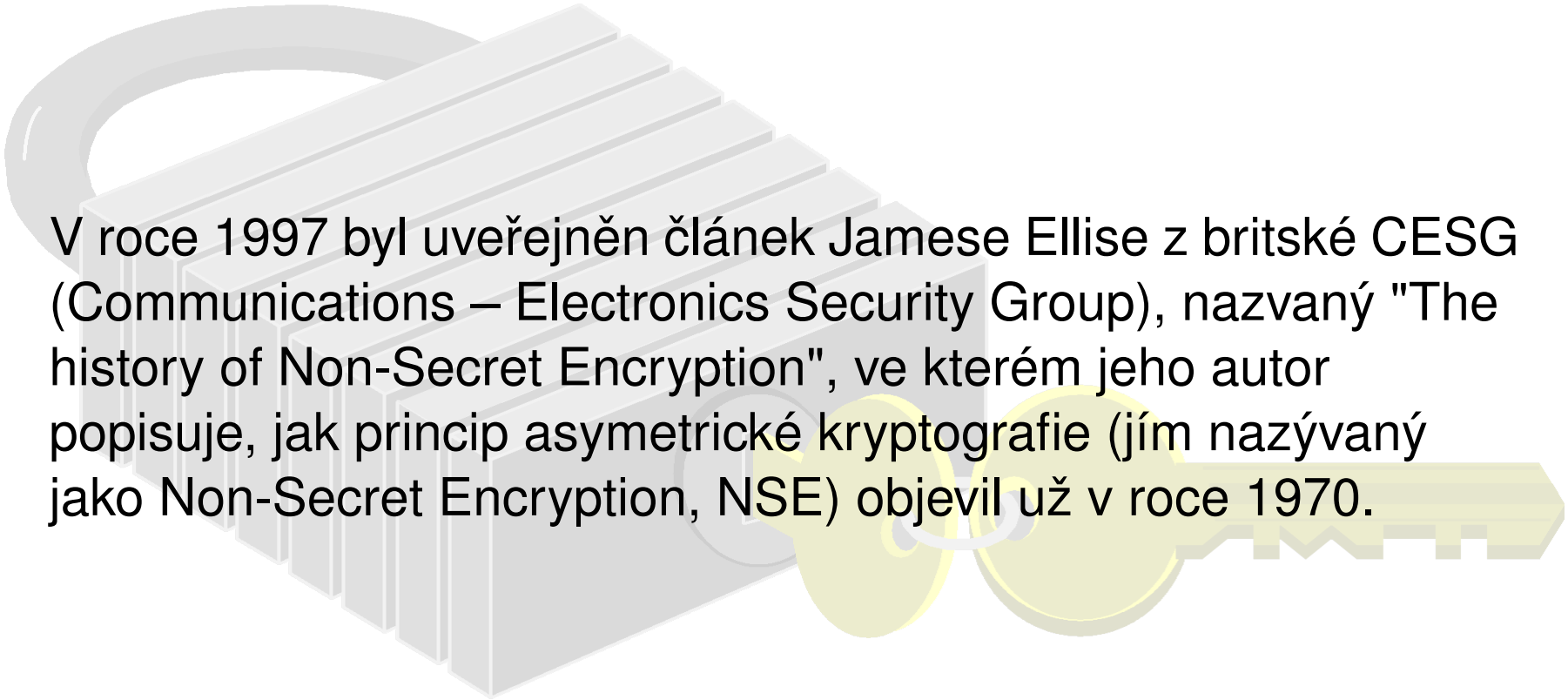
- ***Ron Rivest, Adi Shamir a Len Adleman (1977).***
- ***Založen na neschopnosti lidí faktorizovat velká čísla.***

RSA

- ***Ron Rivest, Adi Shamir a Len Adleman (1977).***
- ***Založen na neschopnosti lidí faktorizovat velká čísla.***
- ***Asymetrické šifrování.***



RSA



V roce 1997 byl uveřejněn článek Jamese Ellise z britské CESG (Communications – Electronics Security Group), nazvaný "The history of Non-Secret Encryption", ve kterém jeho autor popisuje, jak princip asymetrické kryptografie (jím nazývaný jako Non-Secret Encryption, NSE) objevil už v roce 1970.

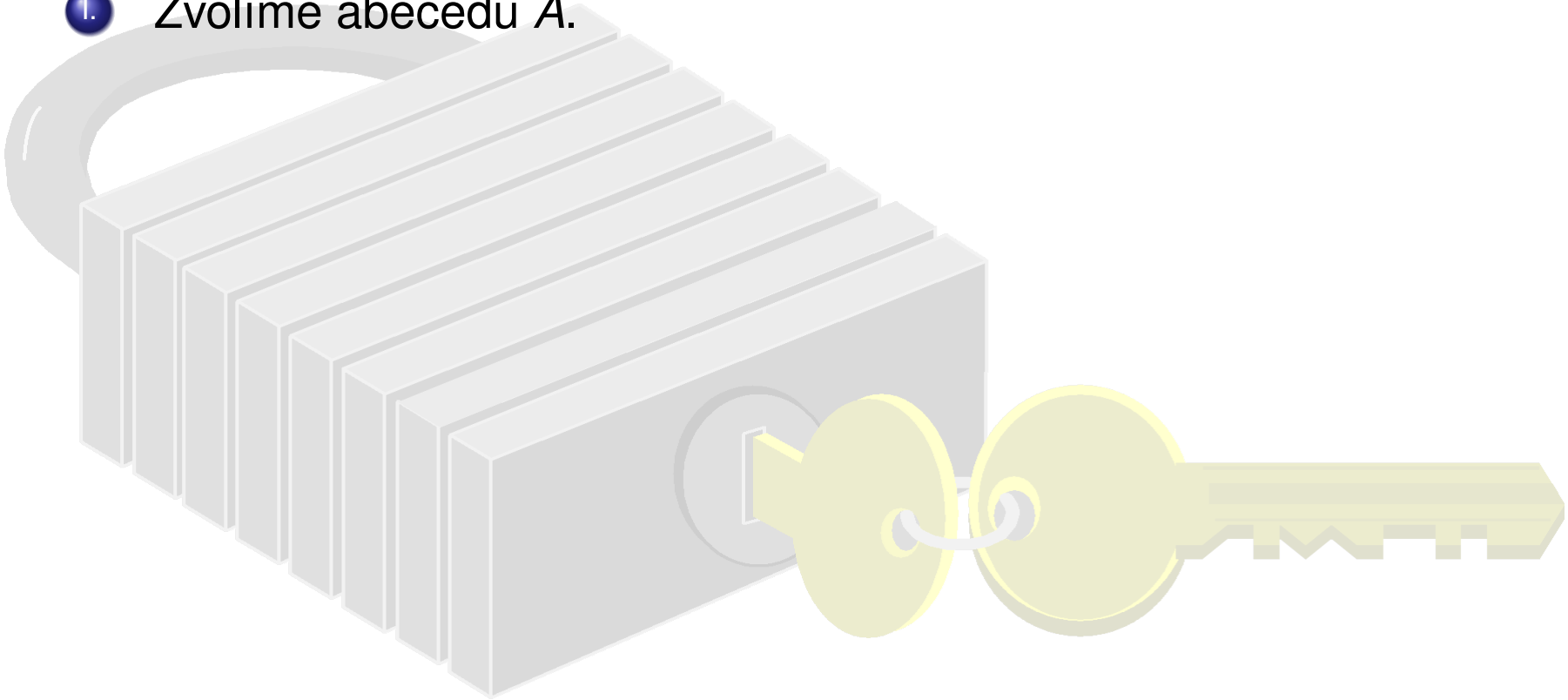
RSA

V roce 1997 byl uveřejněn článek Jamese Ellise z britské CESG (Communications – Electronics Security Group), nazvaný "The history of Non-Secret Encryption", ve kterém jeho autor popisuje, jak princip asymetrické kryptografie (jím nazývaný jako Non-Secret Encryption, NSE) objevil už v roce 1970.

Dále uvádí, že speciální variantu RSA objevil jeho kolega Clifford Cocks v roce 1973.

RSA - Algoritmus

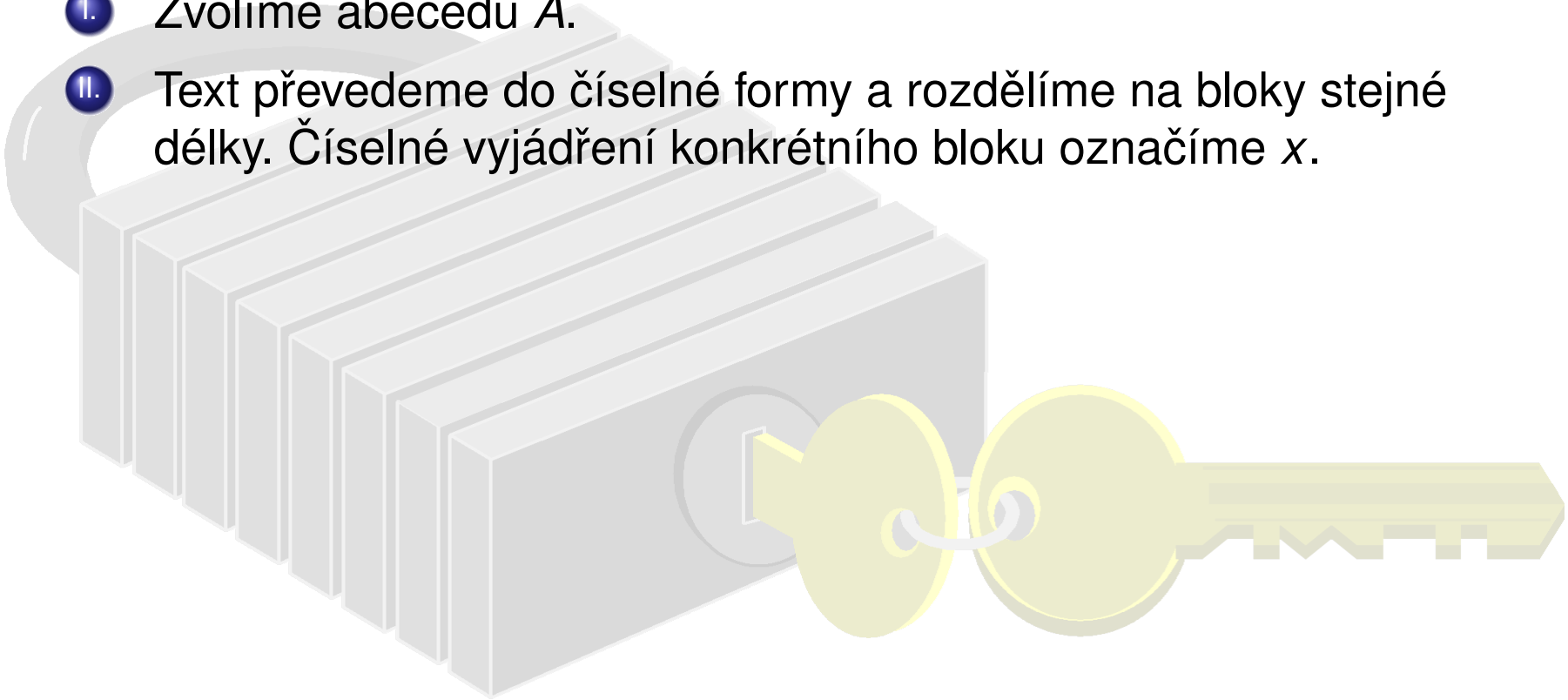
1. Zvolíme abecedu *A*.



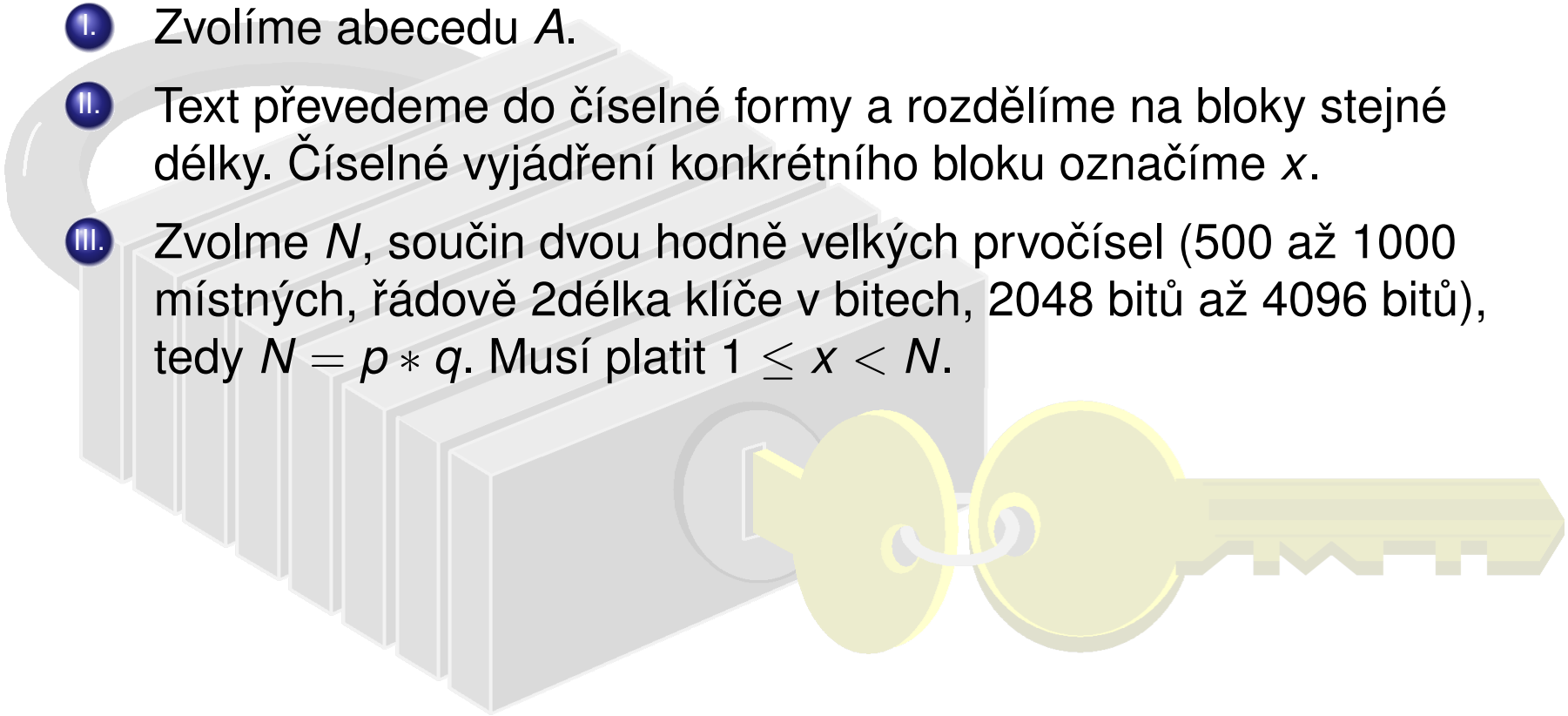
RSA - Algoritmus

I. Zvolíme abecedu A.

II. Text převedeme do číselné formy a rozdělíme na bloky stejné délky. Číselné vyjádření konkrétního bloku označíme x.



RSA - Algoritmus



I. Zvolíme abecedu A.

II. Text převedeme do číselné formy a rozdělíme na bloky stejné délky. Číselné vyjádření konkrétního bloku označíme x.

III. Zvolme N, součin dvou hodně velkých prvočísel (500 až 1000 místných, řádově 2délka klíče v bitech, 2048 bitů až 4096 bitů), tedy $N = p * q$. Musí platit $1 \leq x < N$.

RSA - Algoritmus

I. Zvolíme abecedu A.

II. Text převedeme do číselné formy a rozdělíme na bloky stejné délky. Číselné vyjádření konkrétního bloku označíme x.

III. Zvolme N, součin dvou hodně velkých prvočísel (500 až 1000 místných, řádově 2délka klíče v bitech, 2048 bitů až 4096 bitů), tedy $N = p * q$. Musí platit $1 \leq x < N$.

IV. Zvolíme si tzv. šifrovací exponent s tak, aby byl nesoudělný s funkcí $f(N)$, tj. $d(s, f(N)) = d(s, (p-1) * (q-1)) = 1$, kde $d(a, b)$ je největší společný dělitel.

RSA - Algoritmus

I. Zvolíme abecedu A.

II. Text převedeme do číselné formy a rozdělíme na bloky stejné délky. Číselné vyjádření konkrétního bloku označíme x.

III. Zvolme N, součin dvou hodně velkých prvočísel (500 až 1000 místných, řádově 2délka klíče v bitech, 2048 bitů až 4096 bitů), tedy $N = p * q$. Musí platit $1 \leq x < N$.

IV. Zvolíme si tzv. šifrovací exponent s tak, aby byl nesoudělný s funkcí $f(N)$, tj. $d(s, f(N)) = d(s, (p-1) * (q-1)) = 1$, kde $d(a, b)$ je největší společný dělitel.

V. Každý oznámí dvojici (N, s).

RSA - Algoritmus

I. Zvolíme abecedu A.

II. Text převedeme do číselné formy a rozdělíme na bloky stejné délky. Číselné vyjádření konkrétního bloku označíme x.

III. Zvolme N, součin dvou hodně velkých prvočísel (500 až 1000 místných, řádově 2délka klíče v bitech, 2048 bitů až 4096 bitů), tedy $N = p * q$. Musí platit $1 \leq x < N$.

IV. Zvolíme si tzv. šifrovací exponent s tak, aby byl nesoudělný s funkcí $f(N)$, tj. $d(s, f(N)) = d(s, (p-1) * (q-1)) = 1$, kde $d(a, b)$ je největší společný dělitel.

V. Každý oznámí dvojici (N, s).

VI. Dále najdeme číslo t takové, že $t * s = 1 \ mod \ f(N)$, resp. $t * s = 1 \ mod \ (p-1)(q-1)$. Tedy $t * s + (p-1) * (q-1)l = 1$ pro vhodné l.

RSA - Algoritmus

I. Zvolíme abecedu A.

II. Text převedeme do číselné formy a rozdělíme na bloky stejné délky. Číselné vyjádření konkrétního bloku označíme x.

III. Zvolme N, součin dvou hodně velkých prvočísel (500 až 1000 místných, řádově 2délka klíče v bitech, 2048 bitů až 4096 bitů), tedy $N = p * q$. Musí platit $1 \leq x < N$.

IV. Zvolíme si tzv. šifrovací exponent s tak, aby byl nesoudělný s funkcí $f(N)$, tj. $d(s, f(N)) = d(s, (p-1) * (q-1)) = 1$, kde $d(a, b)$ je největší společný dělitel.

V. Každý oznámí dvojici (N, s).

VI. Dále najdeme číslo t takové, že $t * s = 1 \ mod \ f(N)$, resp. $t * s = 1 \ mod \ (p-1)(q-1)$. Tedy $t * s + (p-1) * (q-1)l = 1$ pro vhodné l.

VII. Šifrujeme $y = xs \ mod \ N$ a dešifrujeme $x = yt \ mod \ N$.

RSA - Příklad

Příklad 5.1

$p, q \ldots$ prvočísla, součin vyšší než nejvyšší zašifrovatelné číslo.

RSA - Příklad

Příklad 5.1

p, q . . . prvočísla, součin vyšší než nejvyšší zašifrovatelné číslo.

N - modul ("část" veřejného klíče):

$N = p \cdot q$ $\qquad$ $N = 3 \cdot 7 = 21$

$f(N) = (p-1) \cdot (q-1)$ $\qquad$ $f(21) = 2 \cdot 6 = 12$

s - šifrovací exponent (veřejný klíč):

zvolme $s < f(N)$, *s je nesoudělné s* $f(N)$ $\qquad$ $s = 5$

t - dešifrovací exponent (soukromý klíč):

zbytek po dělení $s \cdot t / f(N)$ *je 1* $\qquad$ $5 \cdot t/12 = x$, *zbytek 1*

tj. $s \cdot t \bmod f(N) = 1$ $\qquad$ *např.* $t = 17, x = 7$

RSA - Příklad

Příklad 5.1

p, q . . . prvočísla, součin vyšší než nejvyšší zašifrovatelné číslo.

RSA - Příklad

Příklad 5.1

p, q . . . prvočísla, součin vyšší než nejvyšší zašifrovatelné číslo.

zpráva $\ldots 0 < M < N$ *zašifrovaná zpráva* $\ldots C$

$f(N) = (p-1)\cdot(q-1)$ $\underline{f(21) = 2 \cdot 6 = 12}$

Nechť zpráva $M = 2$.

$C = M^e \ mod \ N$ $C = 2^5 \ mod \ 21 = 32 \ mod \ 21 = \underline{11}$

$M = C^d \ mod \ N$ $M = 11^{17} \ mod \ 21$

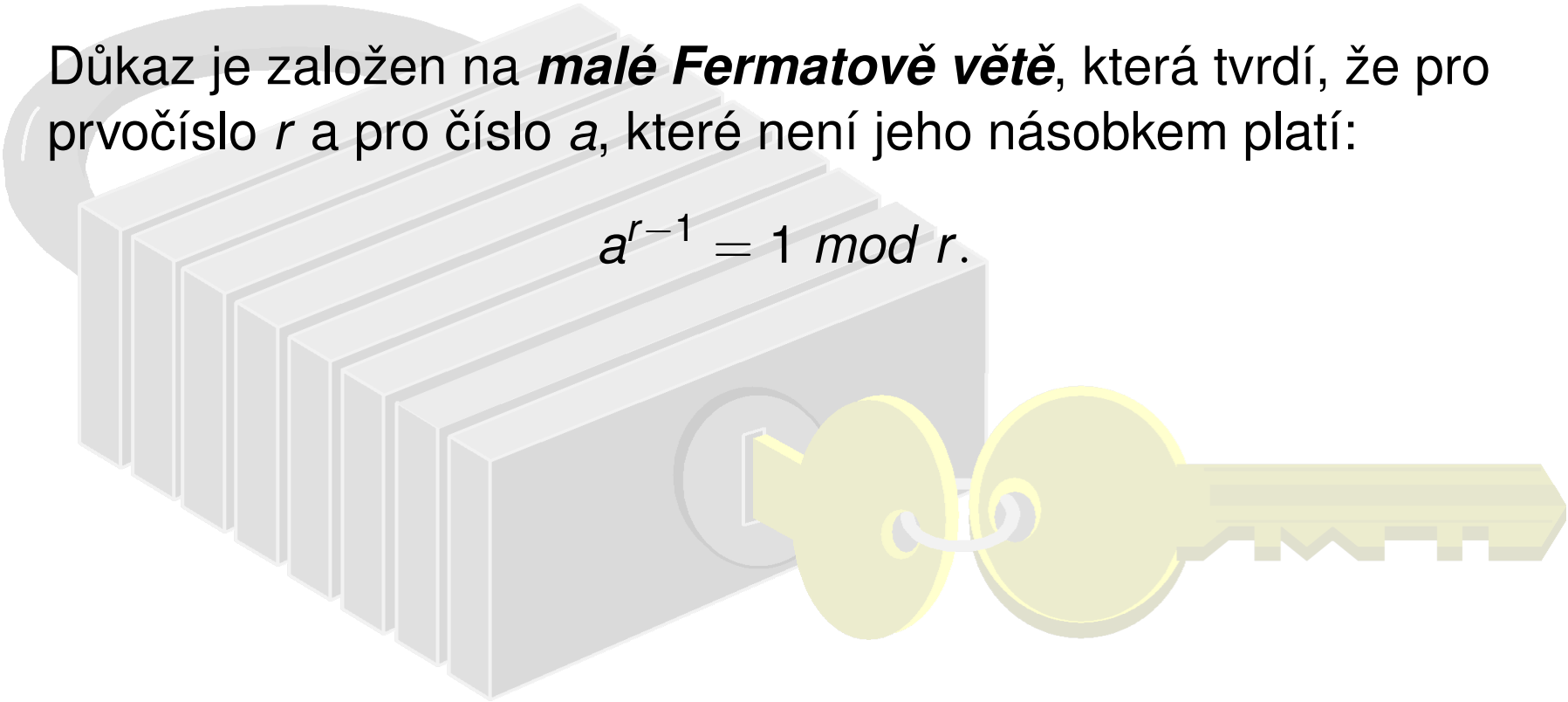
$= 50544702849929377 \ mod \ 21$

$= \underline{2}$

RSA - Korektnost algoritmu

Důkaz je založen na ***malé Fermatově větě***, která tvrdí, že pro prvočíslo r a pro číslo a, které není jeho násobkem platí:

$$a^{r-1} = 1 \ mod \ r.$$



RSA - Korektnost algoritmu

Důkaz je založen na ***malé Fermatově větě***, která tvrdí, že pro prvočíslo r a pro číslo a, které není jeho násobkem platí:

$$a^{r-1} = 1 \ mod \ r.$$

Obecně tedy pro libovolné přirozené číslo k dostáváme

$$a^{k\cdot(r-1)} = 1 \ mod \ r.$$

Dosadíme-li do této rovnice

$$a = x, r = p, k = (q-1)\cdot l$$

dostáváme

$$x^{(p-1)\cdot(r-1)\cdot l} = 1 \ mod \ p.$$

RSA - Korektnost algoritmu

Obdobným dosazením

$$a = x, r = q, k = (p-1) \cdot l$$

dostáváme

$$x^{(p-1)\cdot(r-1)\cdot l} = 1 \ mod \ q.$$

Protože platí $N = p.q$ vychází nám tedy vztah

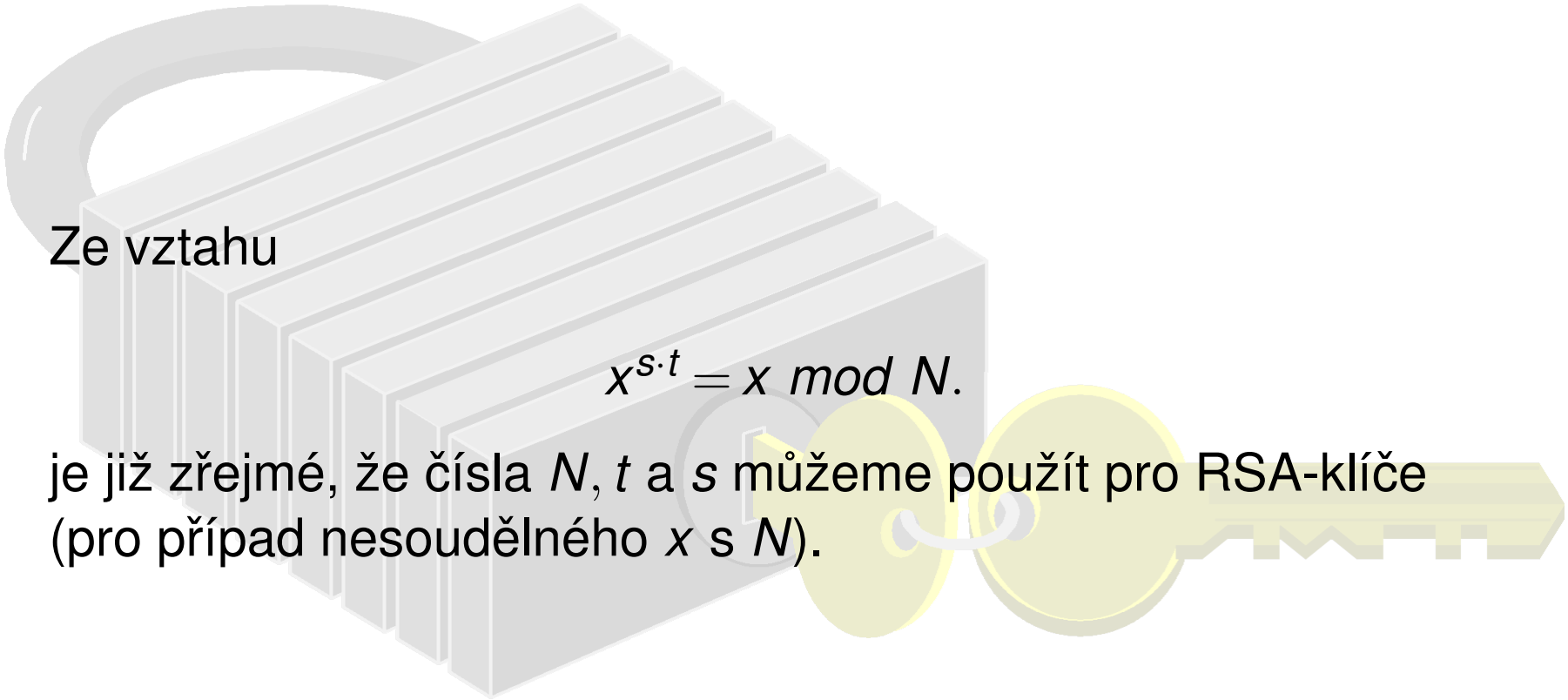
$$x^{(p-1)\cdot(r-1)\cdot l} = 1 \ mod \ N.$$

Nyní již můžeme pomocí předchozí rovnice napsat:

$$x^{s\cdot t} = x^{s\cdot t} \ . \ x^{(p-1)\cdot(r-1)\cdot l}$$

$$= x^{s\cdot t+(p-1)\cdot(r-1)\cdot l} = x^1 = x \ mod \ N.$$

RSA - Korektnost algoritmu

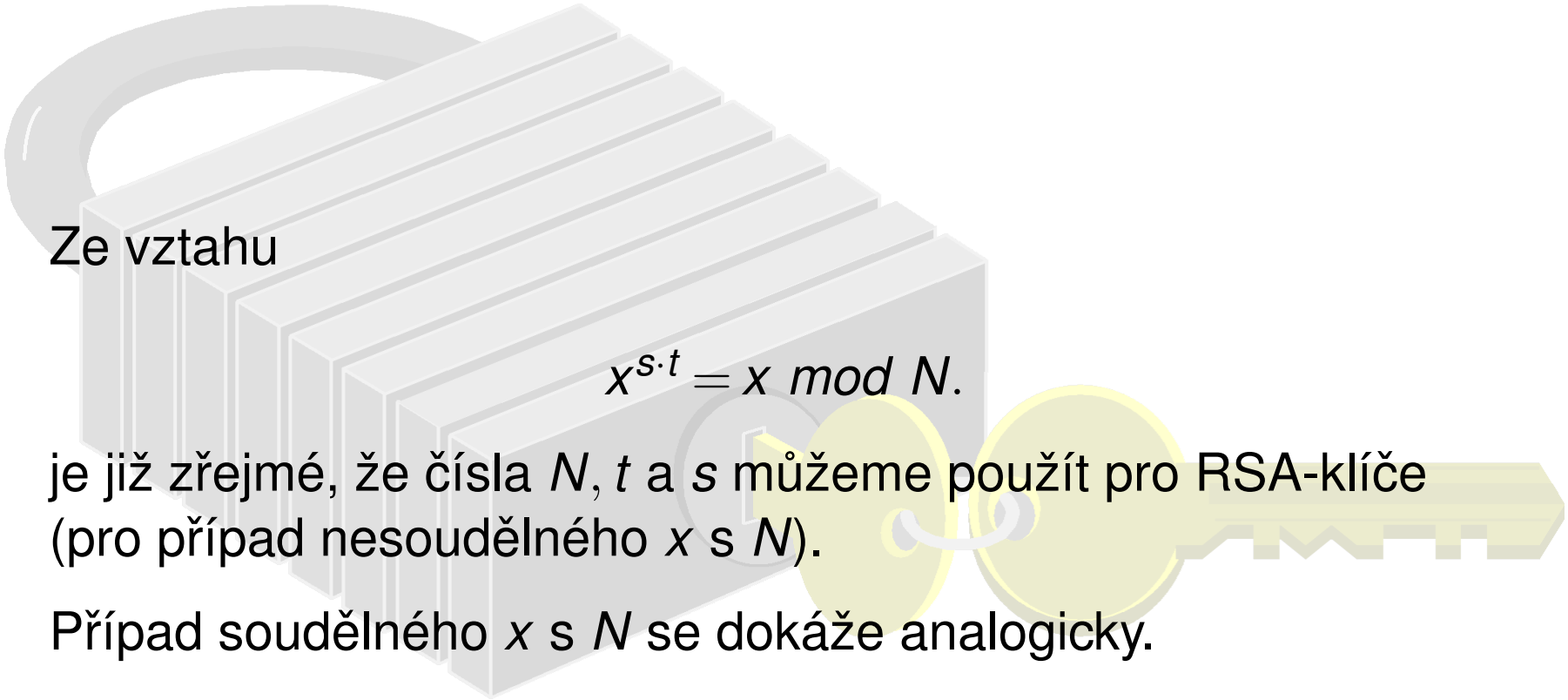


Ze vztahu

$$x^{s \cdot t} = x \ mod \ N.$$

je již zřejmé, že čísla N, t a s můžeme použít pro RSA-klíče (pro případ nesoudělného x s N).

RSA - Korektnost algoritmu



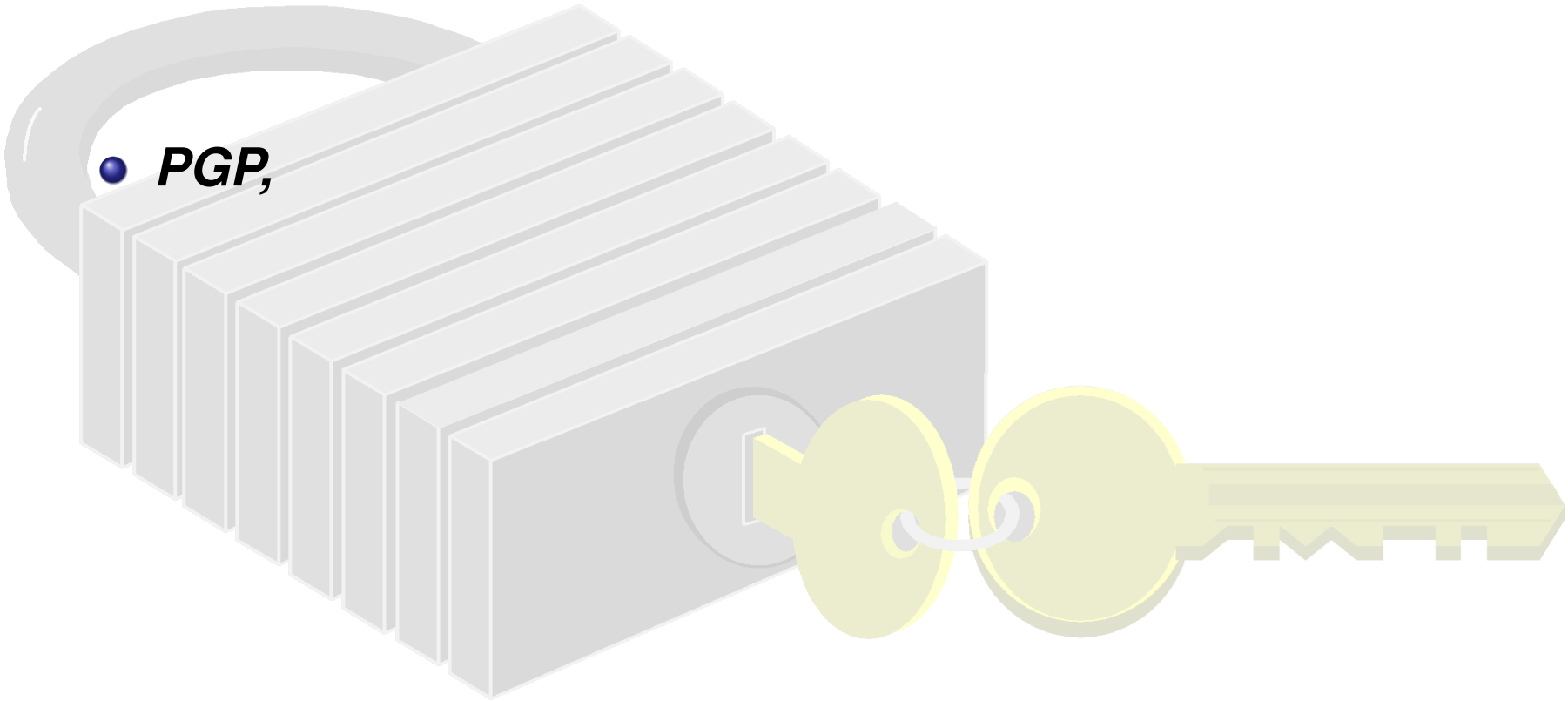
Ze vztahu

$$x^{s \cdot t} = x \ mod \ N.$$

je již zřejmé, že čísla N, t a s můžeme použít pro RSA-klíče (pro případ nesoudělného x s N).

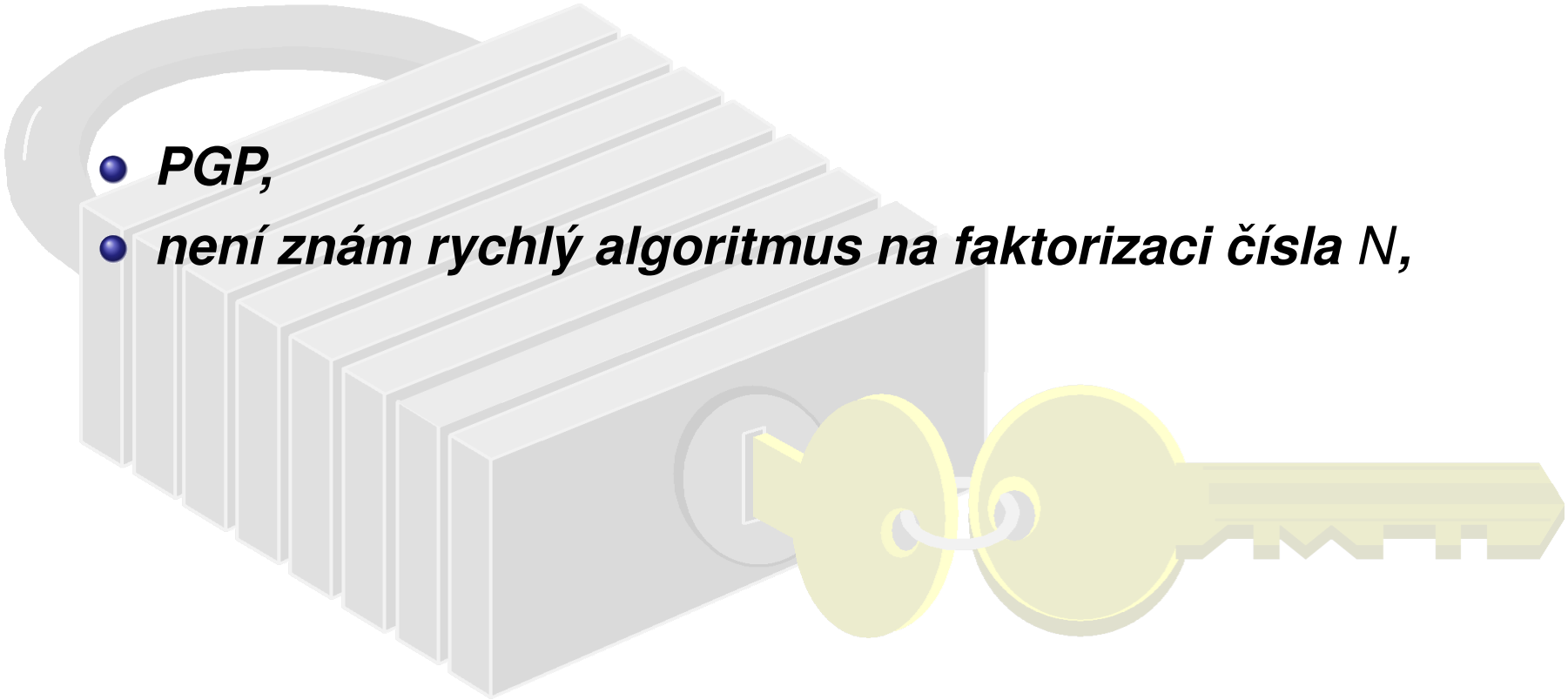
Případ soudělného x s N se dokáže analogicky.

RSA - Využití, bezpečnost, problémy



- ***PGP,***

RSA - Využití, bezpečnost, problémy

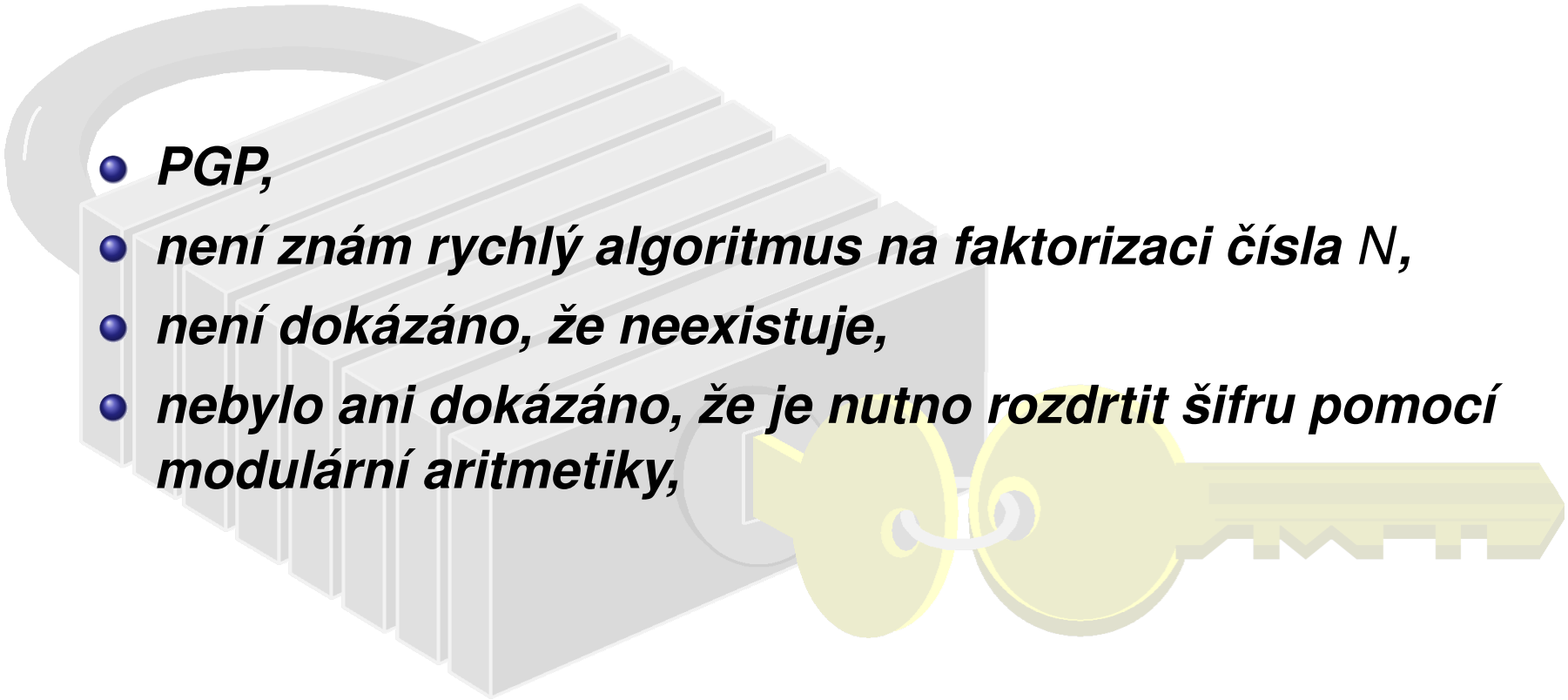


- ***PGP,***
- ***není znám rychlý algoritmus na faktorizaci čísla*** N***,***

RSA - Využití, bezpečnost, problémy

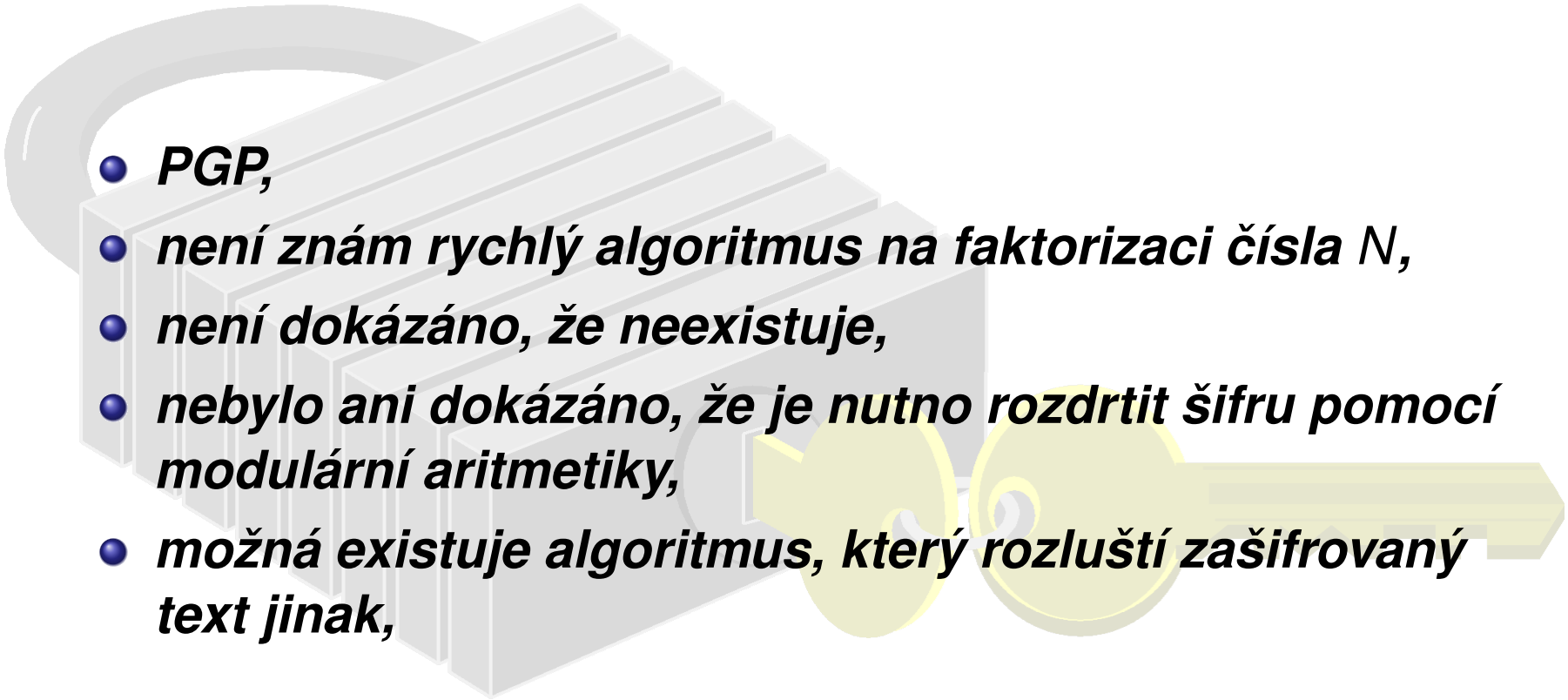
- ***PGP,***
- ***není znám rychlý algoritmus na faktorizaci čísla*** N***,***
- ***není dokázáno, že neexistuje,***

RSA - Využití, bezpečnost, problémy



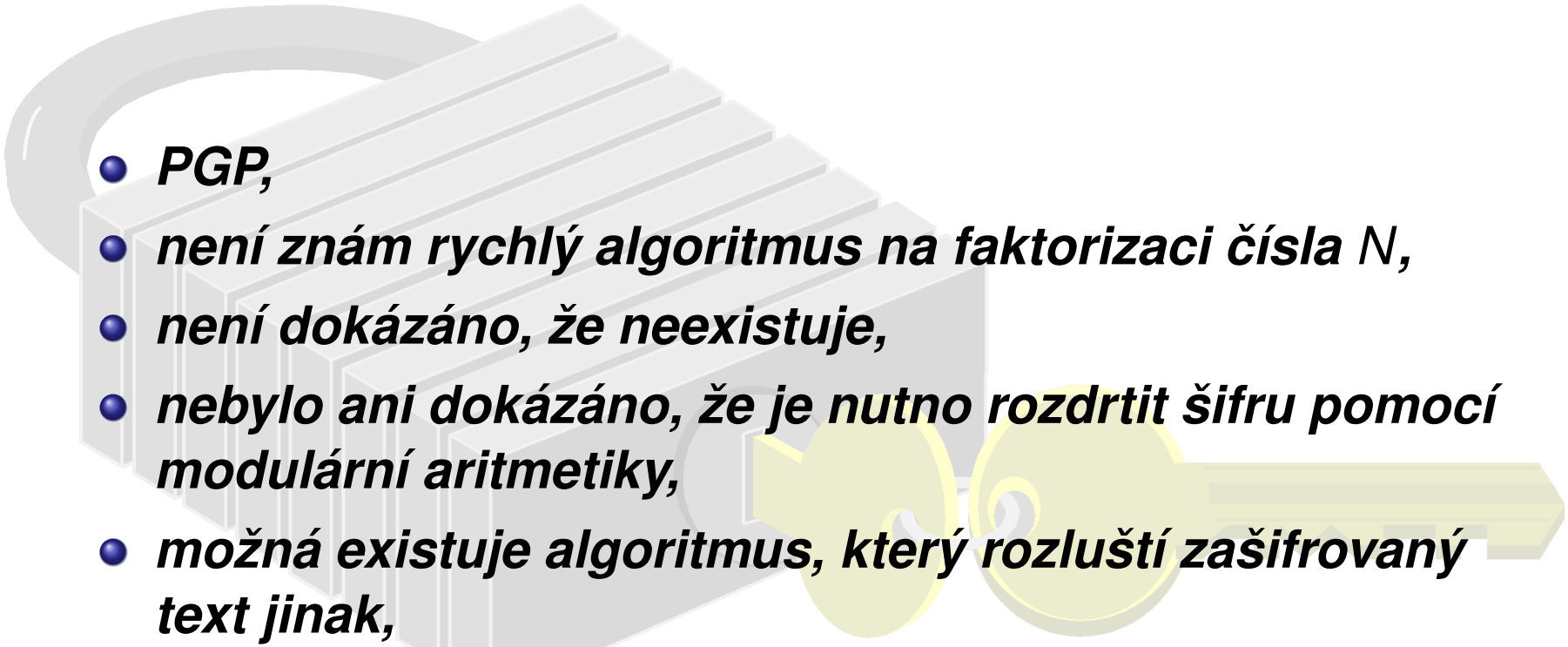
- ***PGP,***
- ***není znám rychlý algoritmus na faktorizaci čísla N,***
- ***není dokázáno, že neexistuje,***
- ***nebylo ani dokázáno, že je nutno rozdrtit šifru pomocí modulární aritmetiky,***

RSA - Využití, bezpečnost, problémy



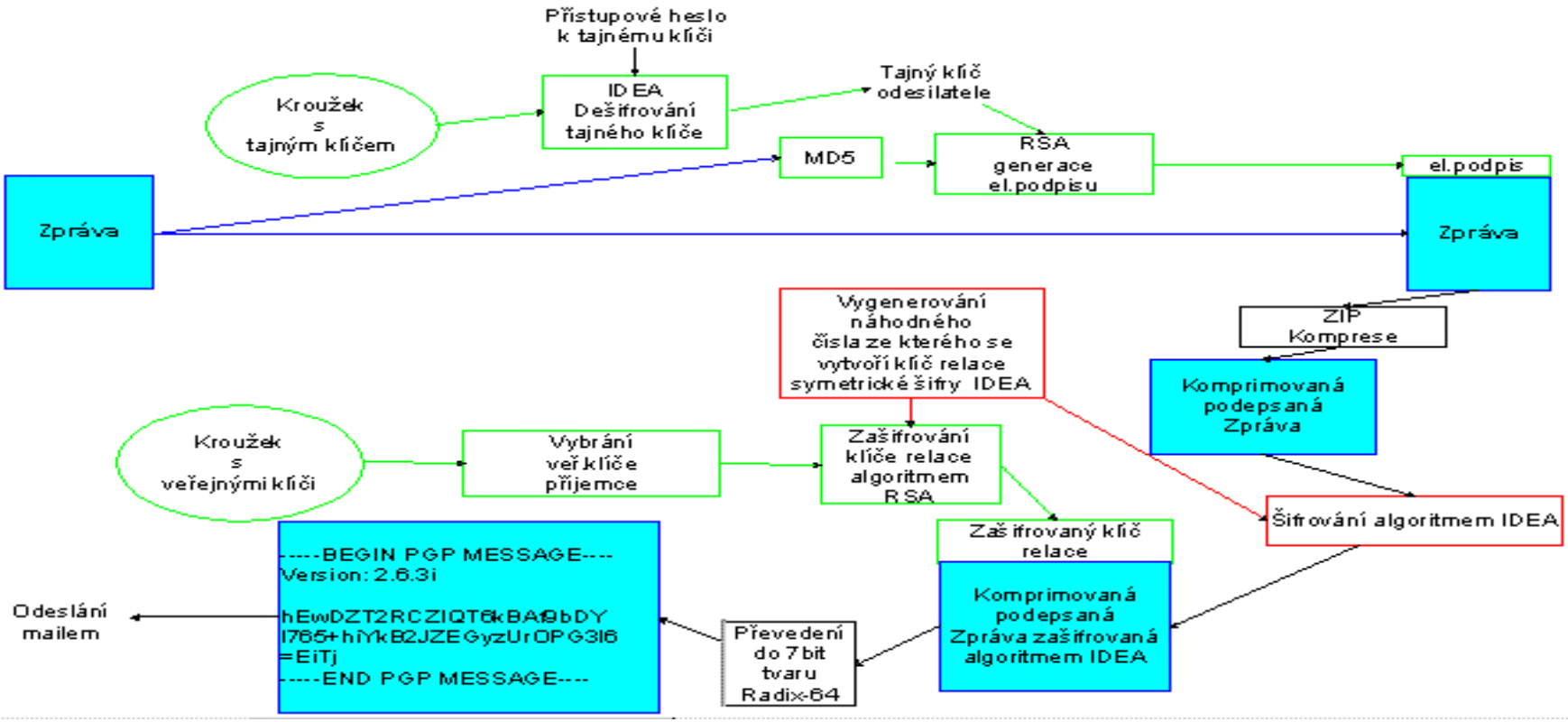
- ***PGP,***
- ***není znám rychlý algoritmus na faktorizaci čísla N,***
- ***není dokázáno, že neexistuje,***
- ***nebylo ani dokázáno, že je nutno rozdrtit šifru pomocí modulární aritmetiky,***
- ***možná existuje algoritmus, který rozluští zašifrovaný text jinak,***

RSA - Využití, bezpečnost, problémy

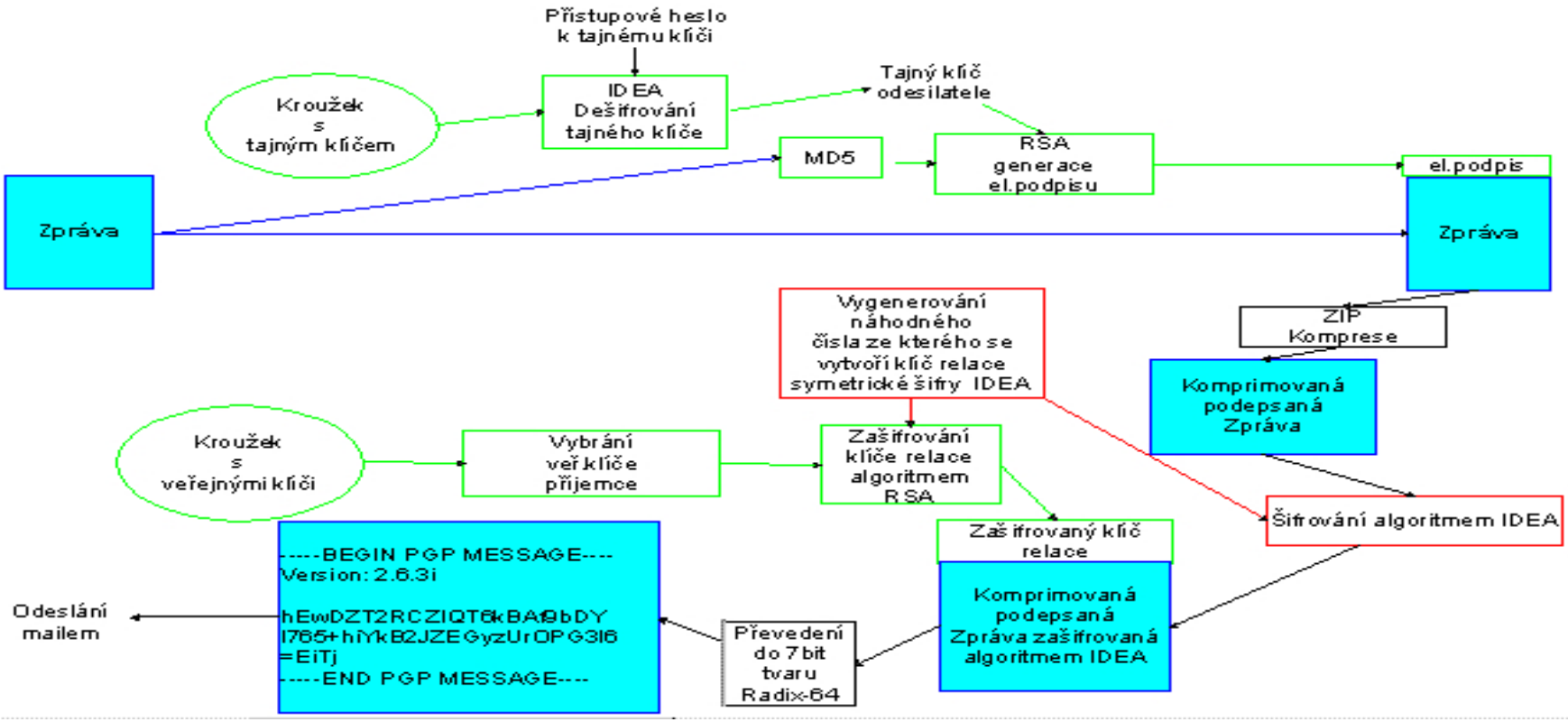


- ***PGP,***
- ***není znám rychlý algoritmus na faktorizaci čísla N,***
- ***není dokázáno, že neexistuje,***
- ***nebylo ani dokázáno, že je nutno rozdrtit šifru pomocí modulární aritmetiky,***
- ***možná existuje algoritmus, který rozluští zašifrovaný text jinak,***
- ***najít dostatečně velká prvočísla p a q je pomalé - hledají se prvočísla s velmi velkou pravděpodobností.***

RSA - PGP


Přístupové heslo k tajnému klíči
Kroužek s tajným klíčem
IDEA Dešifrování tajného klíče
Tajný klíč odesilatele
Zpráva
MD5
RSA generace el.podpisu
el.podpis
Zpráva
Vygenerování náhodného čísla ze kterého se vytvoří klíč relace symetrické šifry IDEA
ZIP Komprese
Komprimovaná podepsaná Zpráva
Kroužek s veřejnými klíči
Vybrání veř.klíče příjemce
Zašifrování klíče relace algoritmem RSA
Šifrování algoritmem IDEA
Zašifrovaný klíč relace
Komprimovaná podepsaná Zpráva zašifrovaná algoritmem IDEA
Odeslání mailem
-----BEGIN PGP MESSAGE-----
Version: 2.6.3i
hEwDZT2RCZIQT6kBA/9bDY
I765+hiYkB2JZEGyzUrOPG3I6
=EiTj
-----END PGP MESSAGE-----
Převedení do 7bit tvaru Radix-64

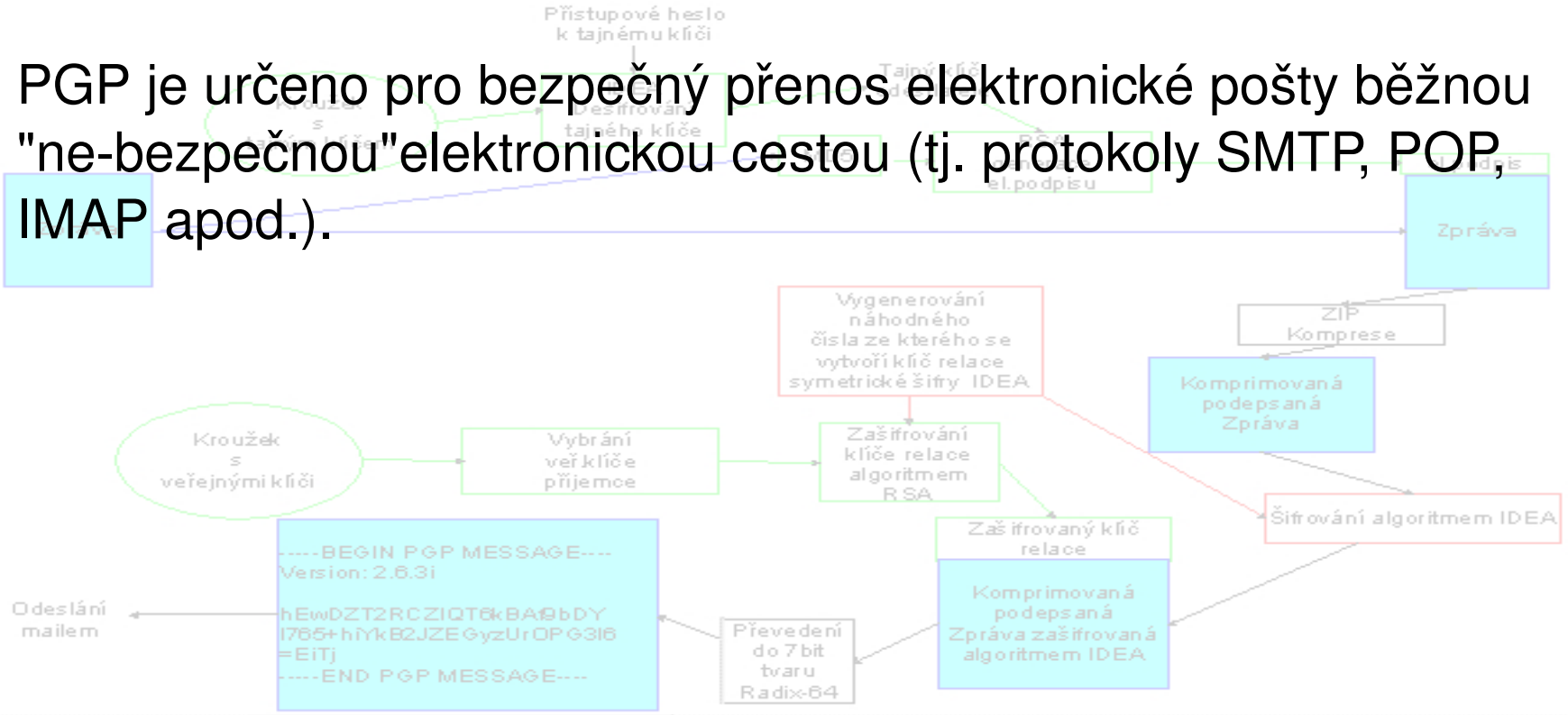
RSA - PGP



PGP (Pretty Good Privacy) vytvořil Američan P.R.Zimmerman. První verze PGP jsou z roku 1991.

RSA - PGP

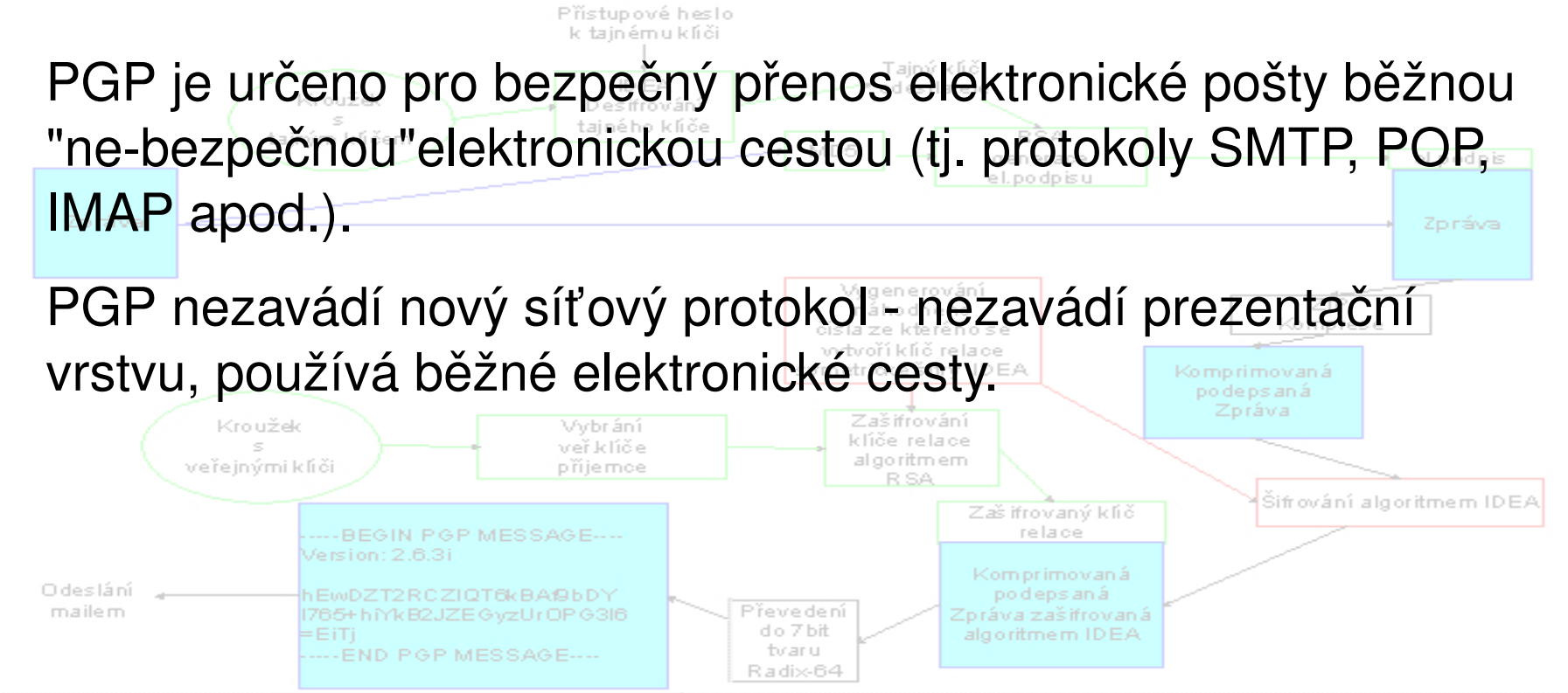
PGP je určeno pro bezpečný přenos elektronické pošty běžnou "ne-bezpečnou"elektronickou cestou (tj. protokoly SMTP, POP, IMAP apod.).



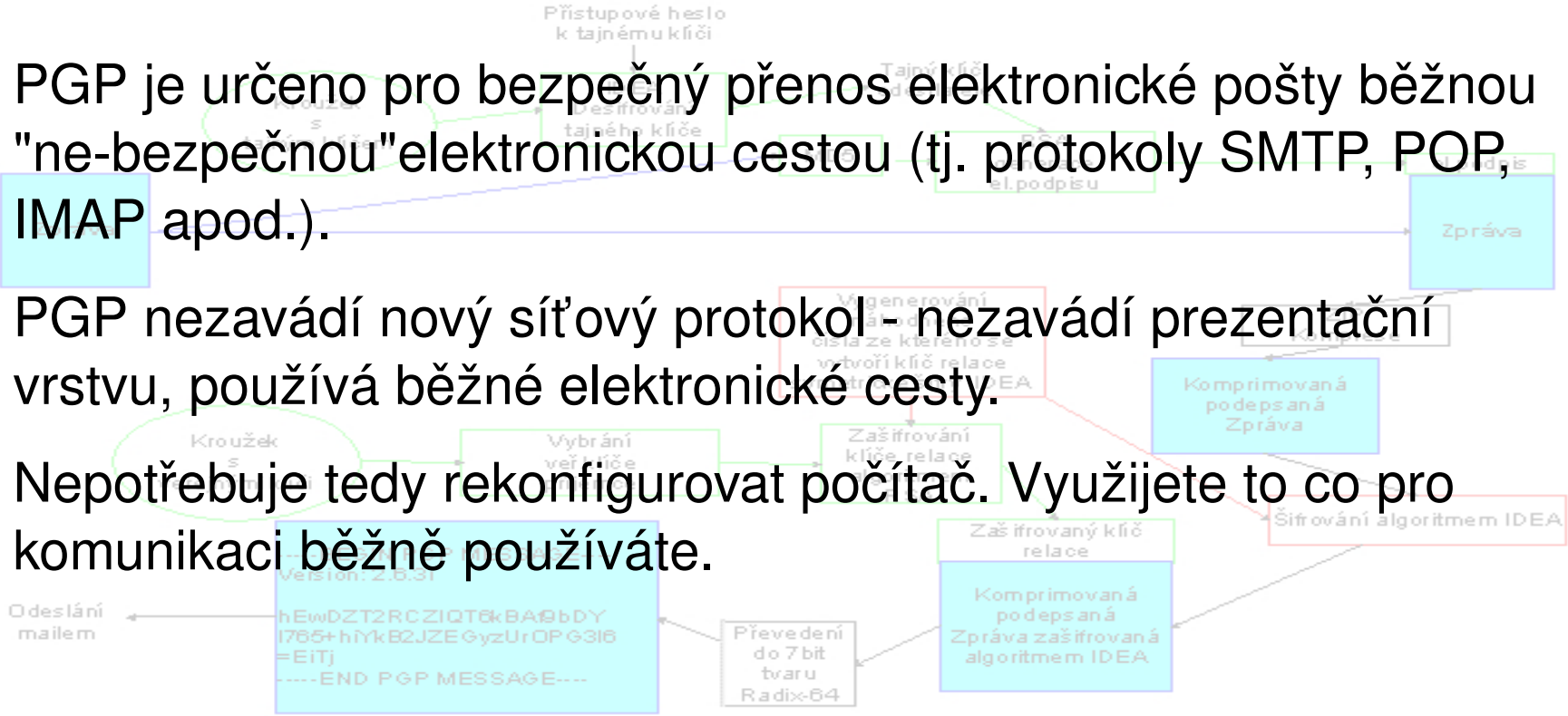
RSA - PGP

PGP je určeno pro bezpečný přenos elektronické pošty běžnou "ne-bezpečnou"elektronickou cestou (tj. protokoly SMTP, POP, IMAP apod.).

PGP nezavádí nový síťový protokol - nezavádí prezentační vrstvu, používá běžné elektronické cesty.



RSA - PGP

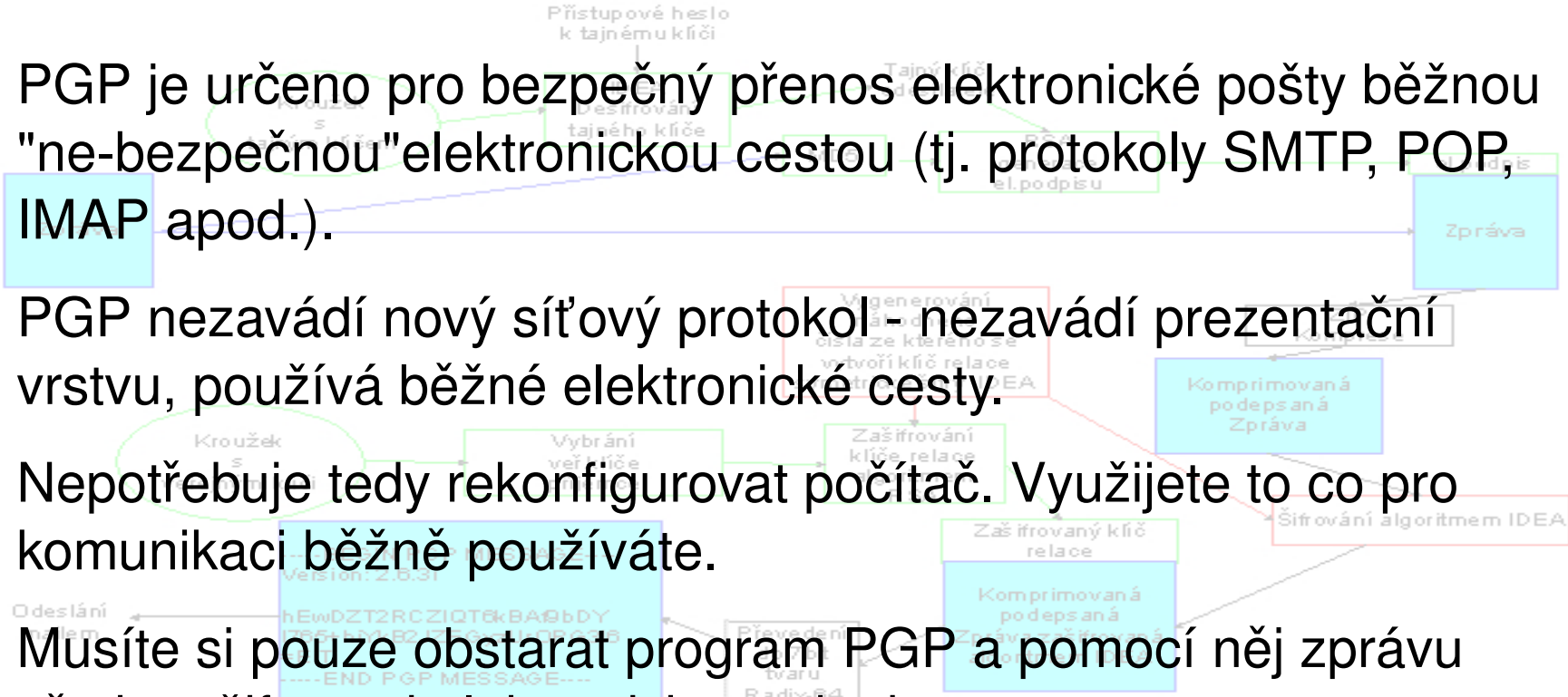


PGP je určeno pro bezpečný přenos elektronické pošty běžnou "ne-bezpečnou"elektronickou cestou (tj. protokoly SMTP, POP, IMAP apod.).

PGP nezavádí nový síťový protokol - nezavádí prezentační vrstvu, používá běžné elektronické cesty.

Nepotřebuje tedy rekonfigurovat počítač. Využijete to co pro komunikaci běžně používáte.

RSA - PGP



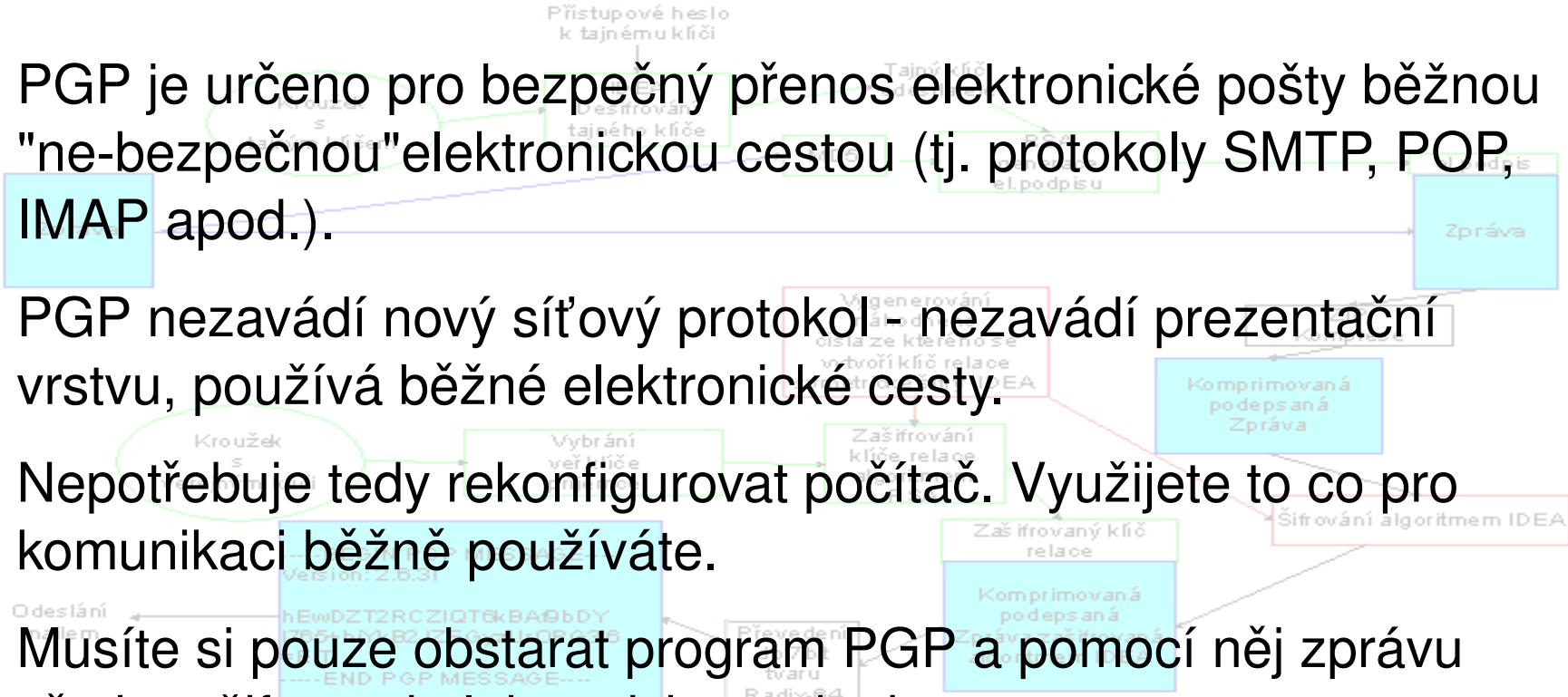
PGP je určeno pro bezpečný přenos elektronické pošty běžnou "ne-bezpečnou"elektronickou cestou (tj. protokoly SMTP, POP, IMAP apod.).

PGP nezavádí nový síťový protokol - nezavádí prezentační vrstvu, používá běžné elektronické cesty.

Nepotřebuje tedy rekonfigurovat počítač. Využijete to co pro komunikaci běžně používáte.

Musíte si pouze obstarat program PGP a pomocí něj zprávu předem šifrovat i elektronicky podepisovat.

RSA - PGP



PGP je určeno pro bezpečný přenos elektronické pošty běžnou "ne-bezpečnou"elektronickou cestou (tj. protokoly SMTP, POP, IMAP apod.).

PGP nezavádí nový síťový protokol - nezavádí prezentační vrstvu, používá běžné elektronické cesty.

Nepotřebuje tedy rekonfigurovat počítač. Využijete to co pro komunikaci běžně používáte.

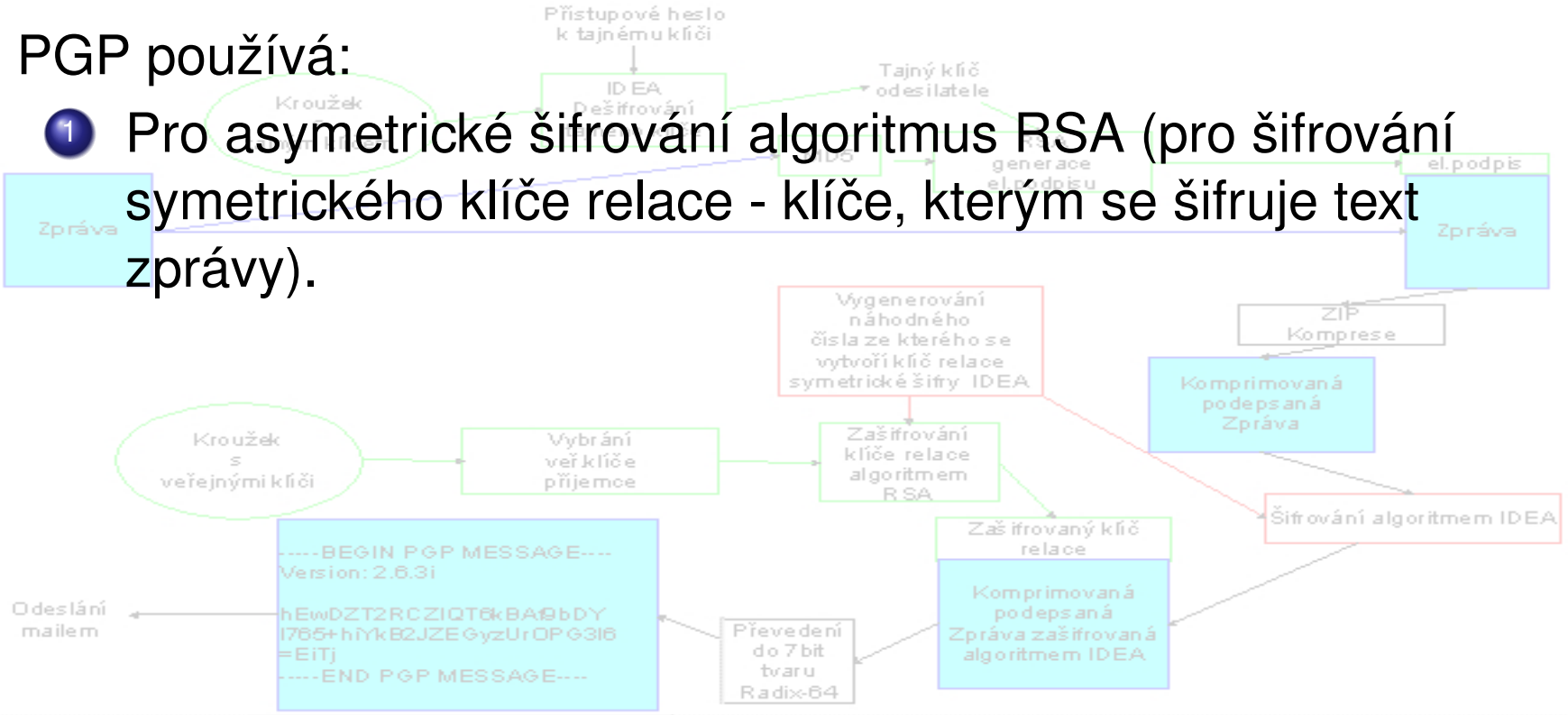
Musíte si pouze obstarat program PGP a pomocí něj zprávu předem šifrovat i elektronicky podepisovat.

Přijatou zprávu je třeba nejprve uložit do souboru, na který se následně aplikuje program PGP.

RSA - PGP

PGP používá:

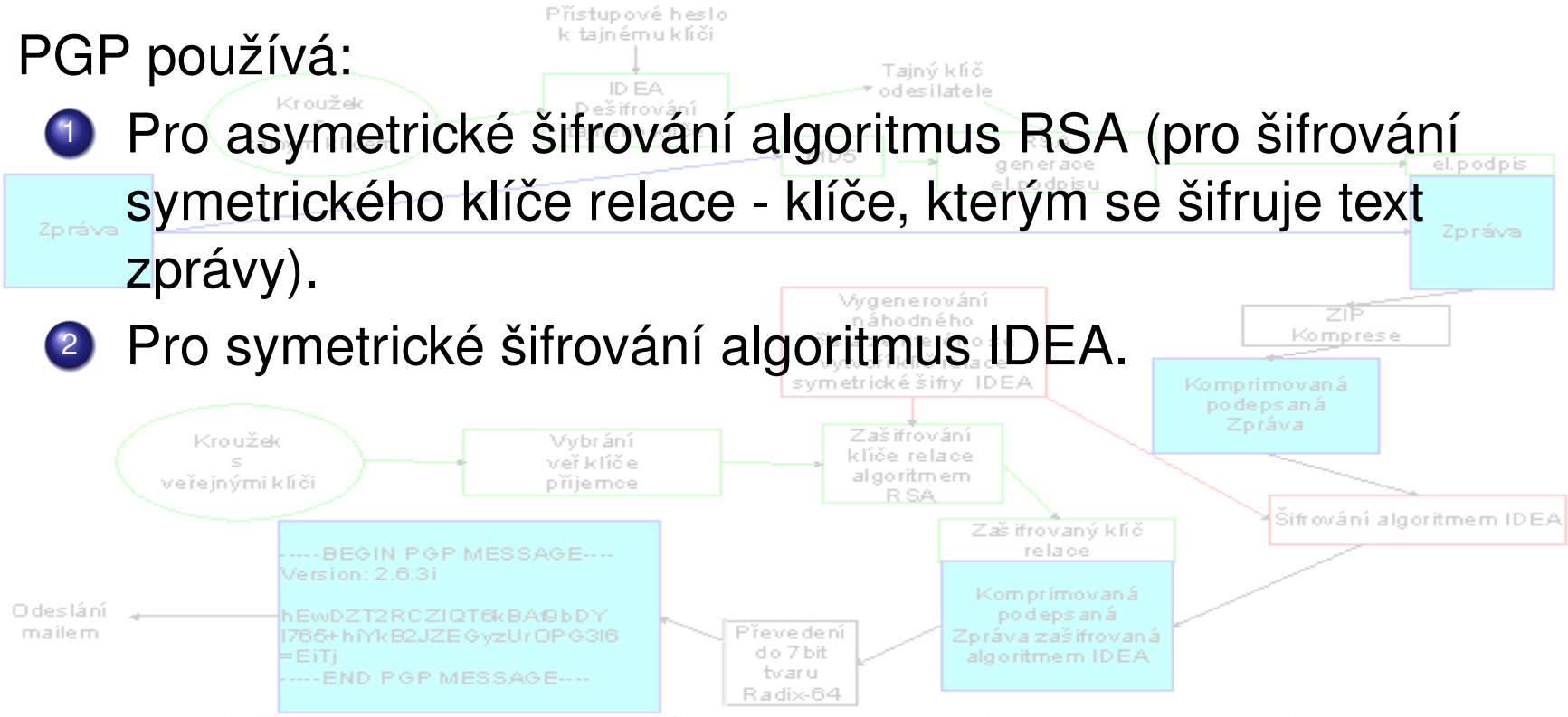
1. Pro asymetrické šifrování algoritmus RSA (pro šifrování symetrického klíče relace - klíče, kterým se šifruje text zprávy).



RSA - PGP

PGP používá:

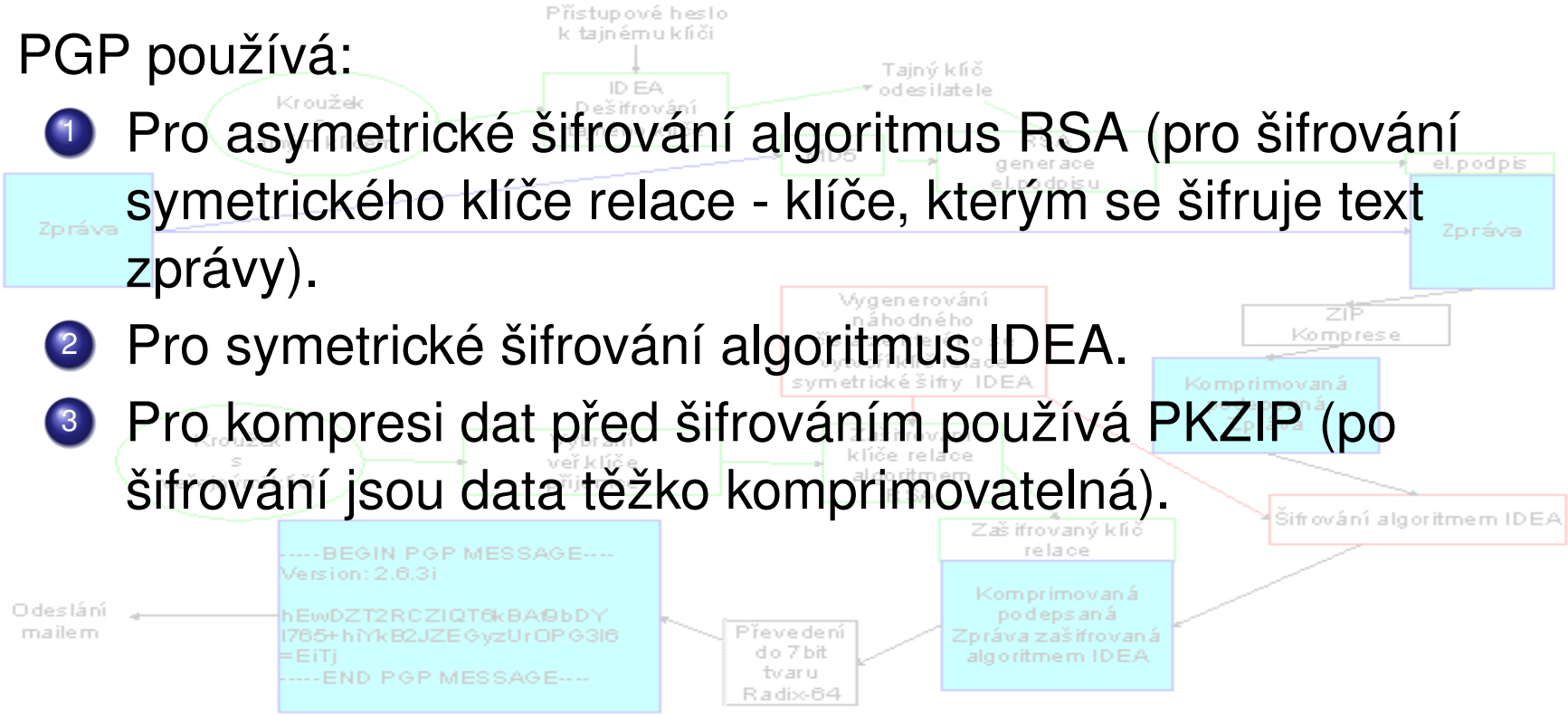
1. Pro asymetrické šifrování algoritmus RSA (pro šifrování symetrického klíče relace - klíče, kterým se šifruje text zprávy).
2. Pro symetrické šifrování algoritmus IDEA.



RSA - PGP

PGP používá:

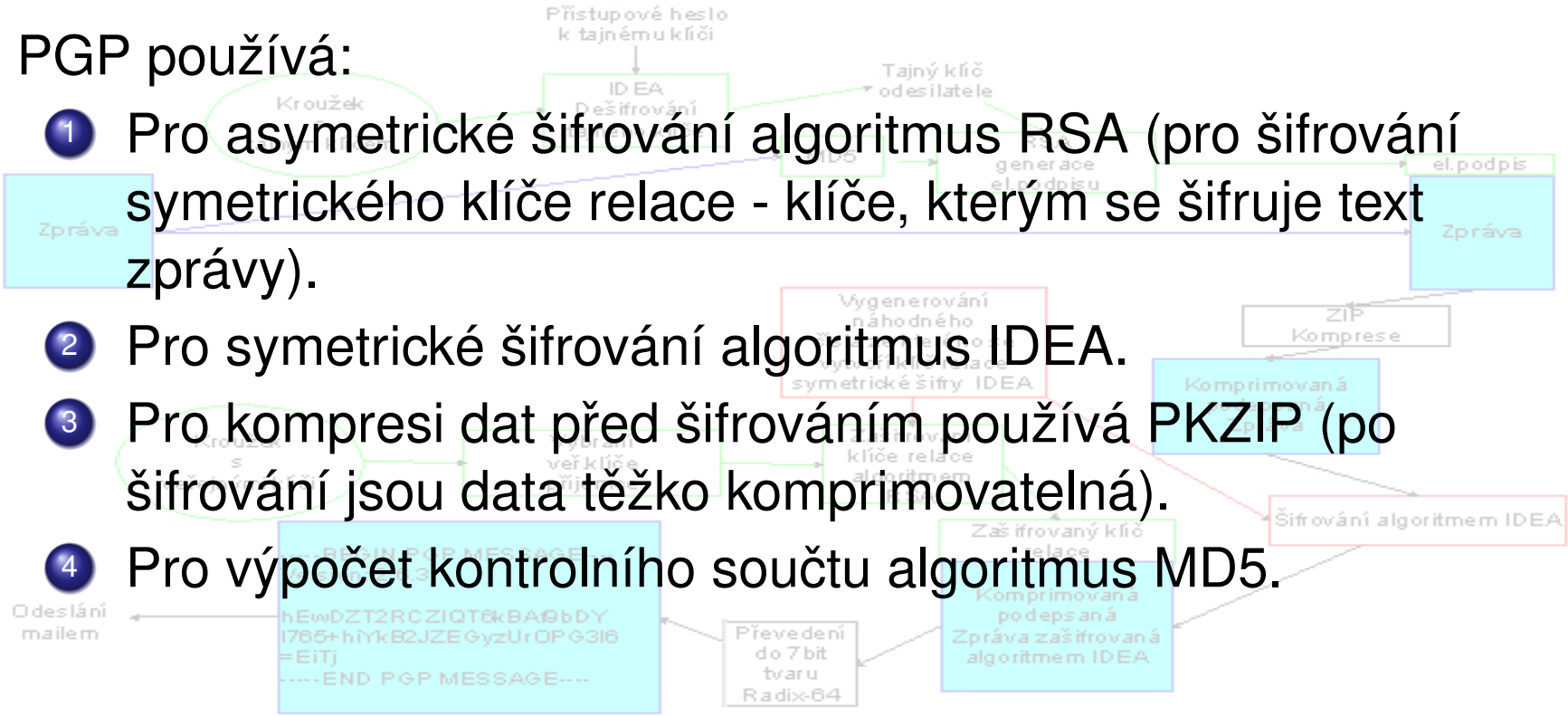
1. Pro asymetrické šifrování algoritmus RSA (pro šifrování symetrického klíče relace - klíče, kterým se šifruje text zprávy).
2. Pro symetrické šifrování algoritmus IDEA.
3. Pro kompresi dat před šifrováním používá PKZIP (po šifrování jsou data těžko komprimovatelná).



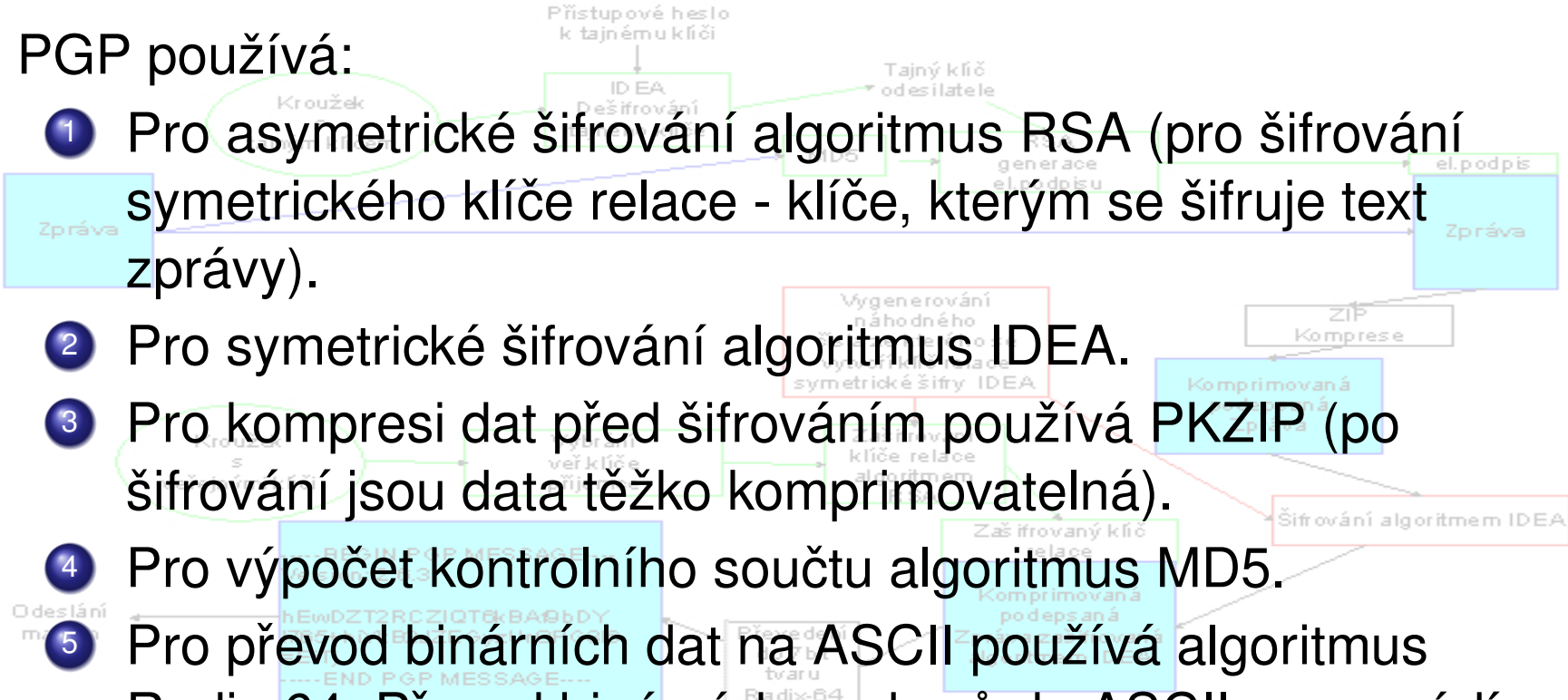
RSA - PGP

PGP používá:

1. Pro asymetrické šifrování algoritmus RSA (pro šifrování symetrického klíče relace - klíče, kterým se šifruje text zprávy).
2. Pro symetrické šifrování algoritmus IDEA.
3. Pro kompresi dat před šifrováním používá PKZIP (po šifrování jsou data těžko komprimovatelná).
4. Pro výpočet kontrolního součtu algoritmus MD5.



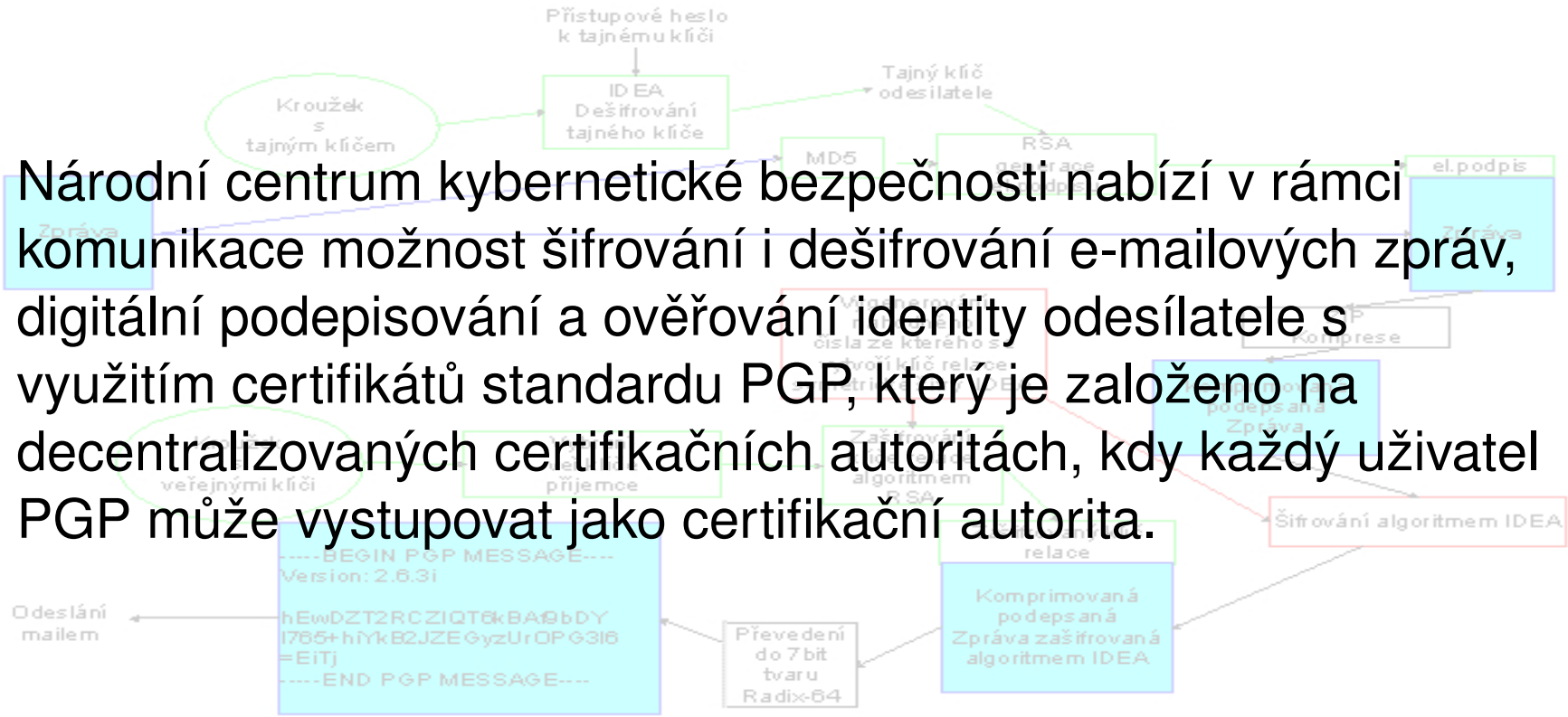
RSA - PGP



PGP používá:

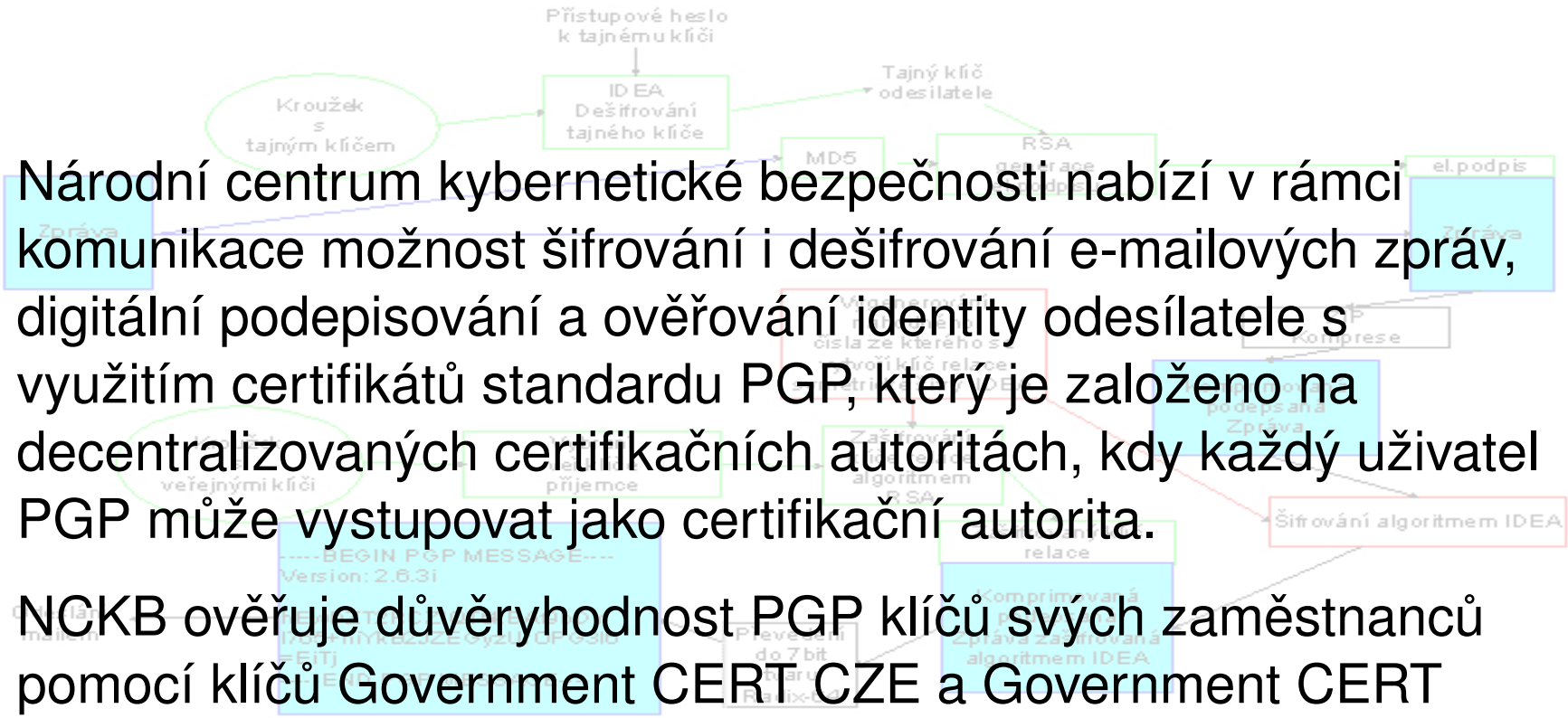
1. Pro asymetrické šifrování algoritmus RSA (pro šifrování symetrického klíče relace - klíče, kterým se šifruje text zprávy).
2. Pro symetrické šifrování algoritmus IDEA.
3. Pro kompresi dat před šifrováním používá PKZIP (po šifrování jsou data těžko komprimovatelná).
4. Pro výpočet kontrolního součtu algoritmus MD5.
5. Pro převod binárních dat na ASCII používá algoritmus Radix-64. Převod binárních souborů do ASCII se provádí proto, aby je bylo možné posílat elektronickou poštou (tj. protokolem SMTP), která je obecně v Internetu jen sedmibitová (tj. ASCII).

RSA - PGP



Národní centrum kybernetické bezpečnosti nabízí v rámci komunikace možnost šifrování i dešifrování e-mailových zpráv, digitální podepisování a ověřování identity odesílatele s využitím certifikátů standardu PGP, který je založeno na decentralizovaných certifikačních autoritách, kdy každý uživatel PGP může vystupovat jako certifikační autorita.

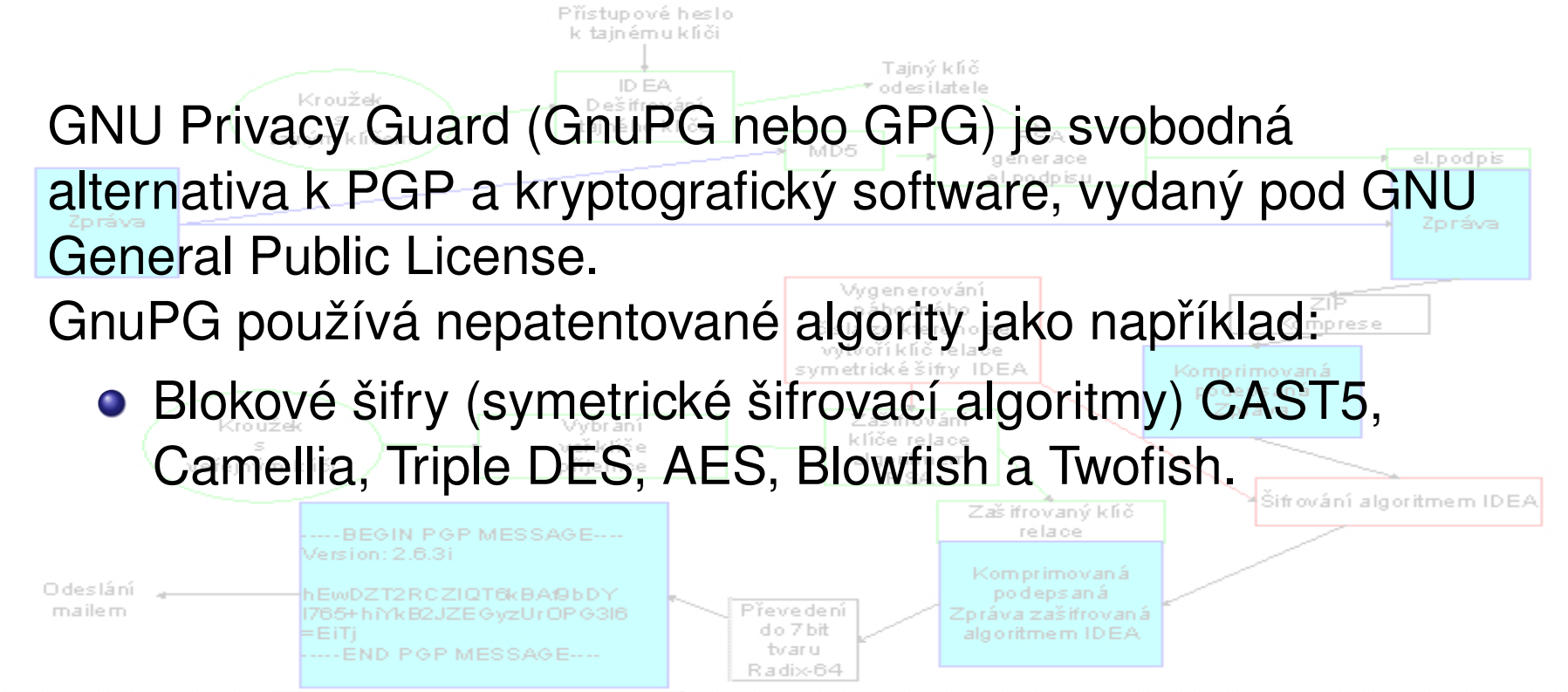
RSA - PGP



Národní centrum kybernetické bezpečnosti nabízí v rámci komunikace možnost šifrování i dešifrování e-mailových zpráv, digitální podepisování a ověřování identity odesílatele s využitím certifikátů standardu PGP, který je založeno na decentralizovaných certifikačních autoritách, kdy každý uživatel PGP může vystupovat jako certifikační autorita.

NCKB ověřuje důvěryhodnost PGP klíčů svých zaměstnanců pomocí klíčů Government CERT CZE a Government CERT Incident CZE.

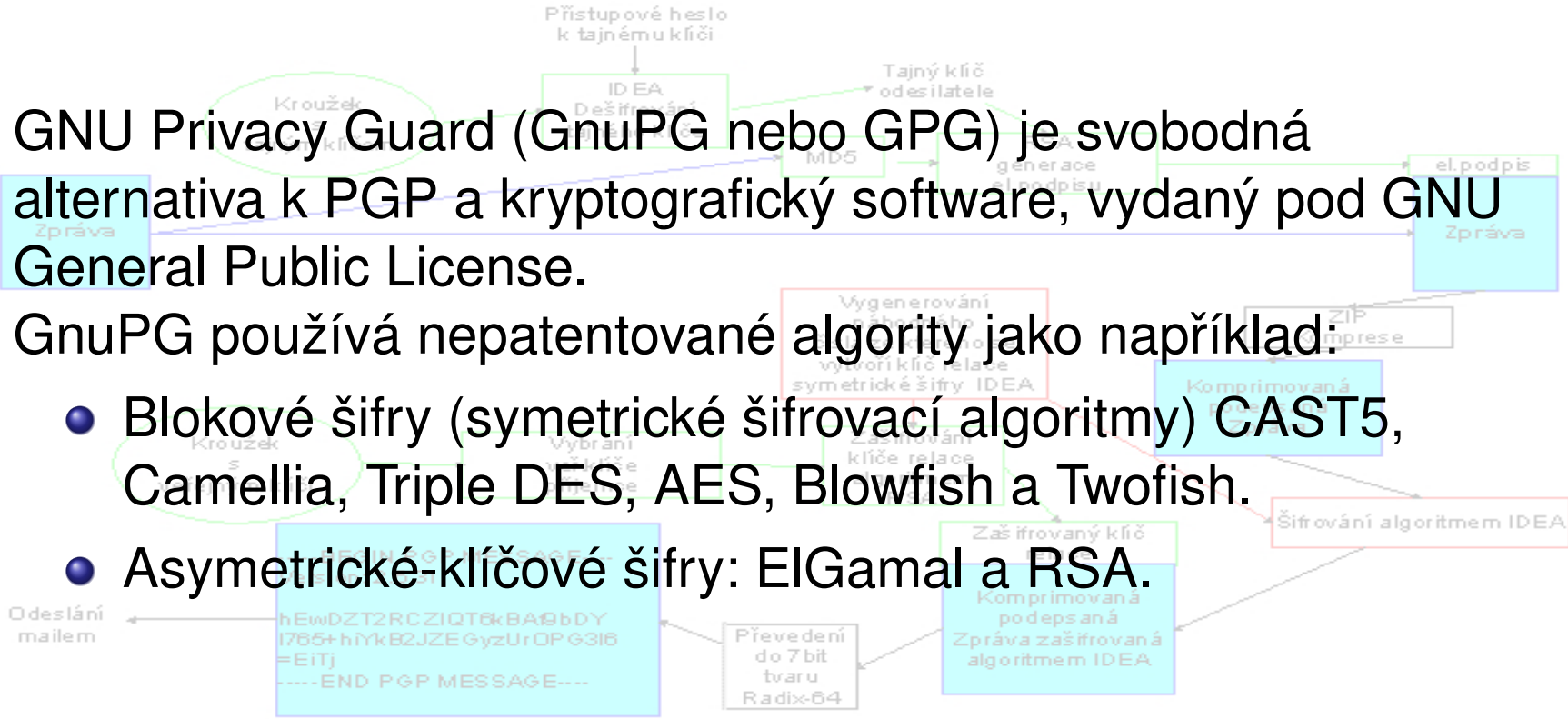
GNU Privacy Guard



GNU Privacy Guard (GnuPG nebo GPG) je svobodná alternativa k PGP a kryptografický software, vydaný pod GNU General Public License.
GnuPG používá nepatentované algority jako například:

- Blokové šifry (symetrické šifrovací algoritmy) CAST5, Camellia, Triple DES, AES, Blowfish a Twofish.

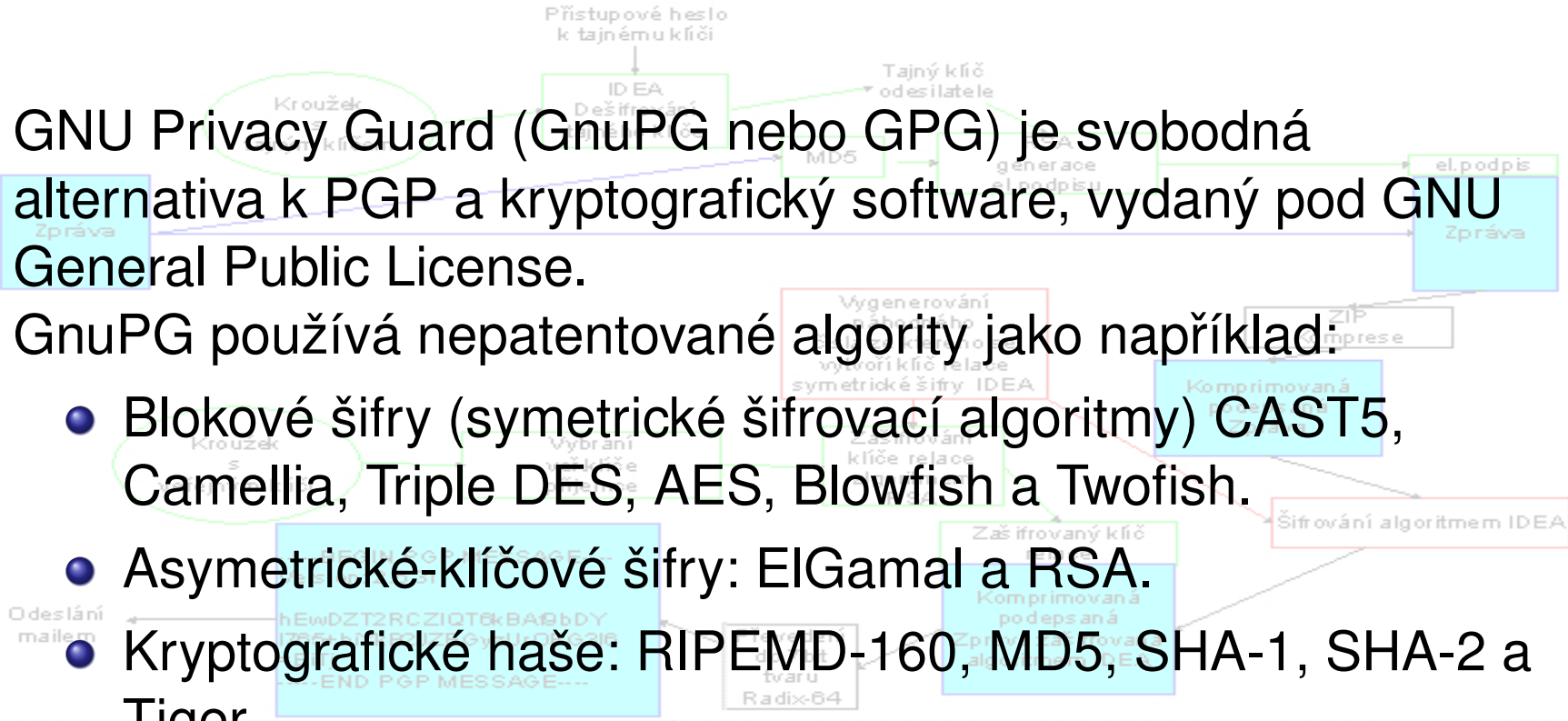
GNU Privacy Guard



GNU Privacy Guard (GnuPG nebo GPG) je svobodná alternativa k PGP a kryptografický software, vydaný pod GNU General Public License.
GnuPG používá nepatentované algority jako například:

- Blokové šifry (symetrické šifrovací algoritmy) CAST5, Camellia, Triple DES, AES, Blowfish a Twofish.
- Asymetrické-klíčové šifry: ElGamal a RSA.

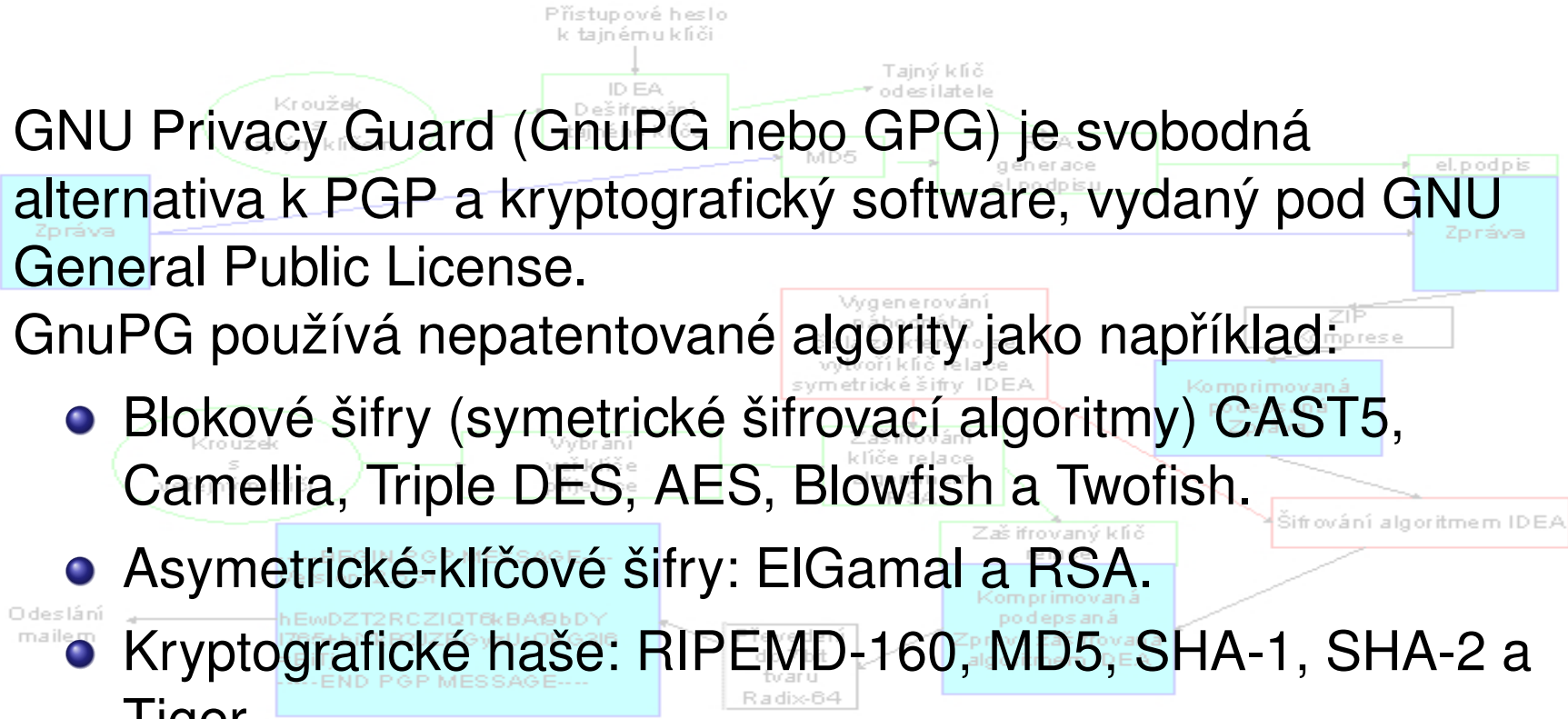
GNU Privacy Guard



GNU Privacy Guard (GnuPG nebo GPG) je svobodná alternativa k PGP a kryptografický software, vydaný pod GNU General Public License.
GnuPG používá nepatentované algority jako například:

- Blokové šifry (symetrické šifrovací algoritmy) CAST5, Camellia, Triple DES, AES, Blowfish a Twofish.
- Asymetrické-klíčové šifry: ElGamal a RSA.
- Kryptografické haše: RIPEMD-160, MD5, SHA-1, SHA-2 a Tiger.

GNU Privacy Guard



GNU Privacy Guard (GnuPG nebo GPG) je svobodná alternativa k PGP a kryptografický software, vydaný pod GNU General Public License.
GnuPG používá nepatentované algority jako například:

- Blokové šifry (symetrické šifrovací algoritmy) CAST5, Camellia, Triple DES, AES, Blowfish a Twofish.
- Asymetrické-klíčové šifry: ElGamal a RSA.
- Kryptografické haše: RIPEMD-160, MD5, SHA-1, SHA-2 a Tiger.
- Digitální podpisy: DSA a RSA.

Kvantová kryptografie

Kvantová kryptografie řeší problém distribuce kryptografického klíče.

Kvantová kryptografie

Kvantová kryptografie řeší problém distribuce kryptografického klíče.

Neumí sice odposlechu zabránit, ale umožňuje spolehlivě zjistit, zda k odposlechu došlo.

Kvantová kryptografie

Kvantová kryptografie řeší problém distribuce kryptografického klíče.

Neumí sice odposlechu zabránit, ale umožňuje spolehlivě zjistit, zda k odposlechu došlo.

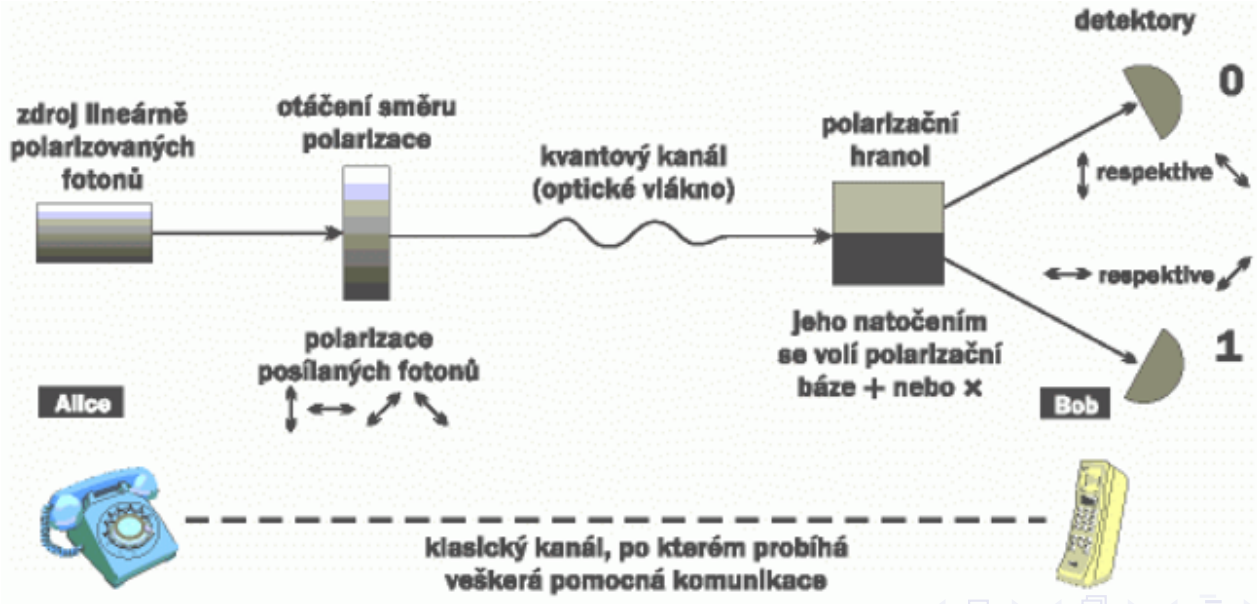
A to v případě přenosu klíče úplně stačí.

Kvantová kryptografie

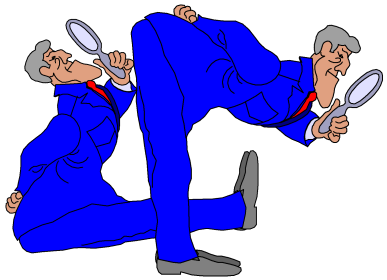
Kvantová kryptografie řeší problém distribuce kryptografického klíče.

Neumí sice odposlechu zabránit, ale umožňuje spolehlivě zjistit, zda k odposlechu došlo.

A to v případě přenosu klíče úplně stačí.



O čem to bude



Zdroje

- www.google.com,
- https://www2.karlin.mff.cuni.cz/ tuma/nciphers12.htm,
- http://www.nist.gov,
- http://www.cacr.math.uwaterloo.ca/hac.