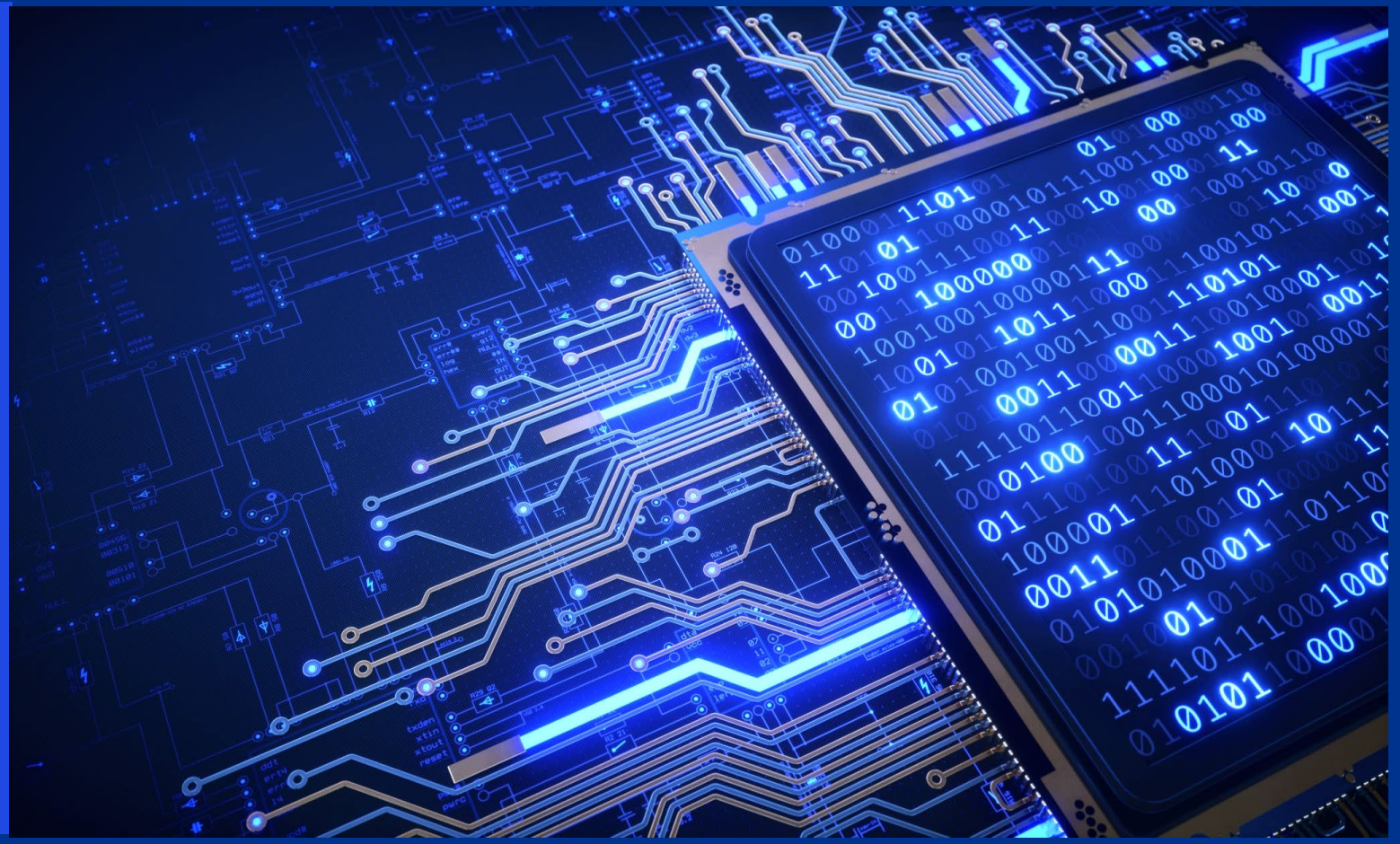
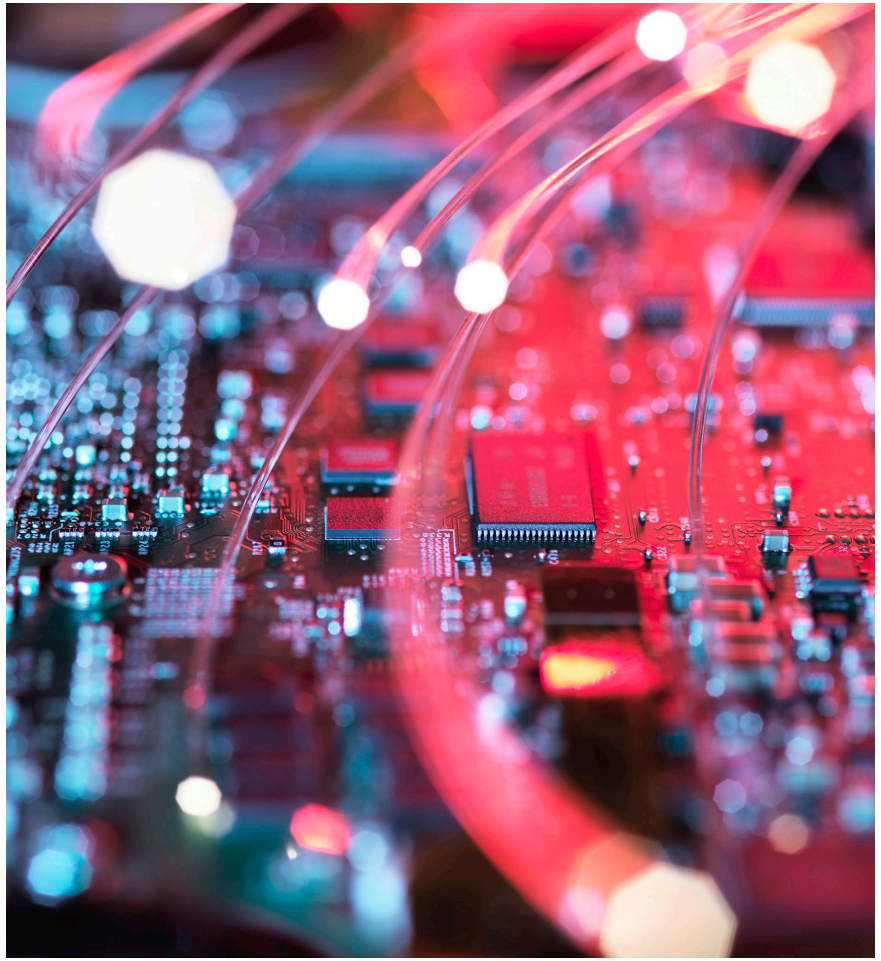
KPMG

PQC - Můžeme zůstat v bezpečí?





Obsah

01

O společnosti KPMG

KPMG Česká republika

KPMG Česká republika zahájila svou činnost v roce 1990, v současné době má více než 1100 zaměstnanců a kanceláře v Praze, Brně, Českých Budějovicích a Ostravě. Společnost poskytuje služby v oblasti auditu, daní, poradenství a práva.

KPMG je celosvětová síť poradenských společností poskytujících služby v oblasti auditu, daní a poradenství. V jejích členských společnostech pracuje více než 236 tisíc odborníků, kteří působí ve 144 státech světa.

Při poskytování služeb našim klientům využíváme informace z celosvětové sítě KPMG, zúročujeme naše odborné znalosti a používáme nejnovější nástroje pro sdílení znalostí, informací
a pro komunikaci.

Naše klienty pravidelně informujeme o aktuálním vývoji na finančních trzích, upozorňujeme je na nové účetní a daňové předpisy a komentujeme dopad legislativy na podnikání. Na požádání vám budeme zasílat tyto publikace:

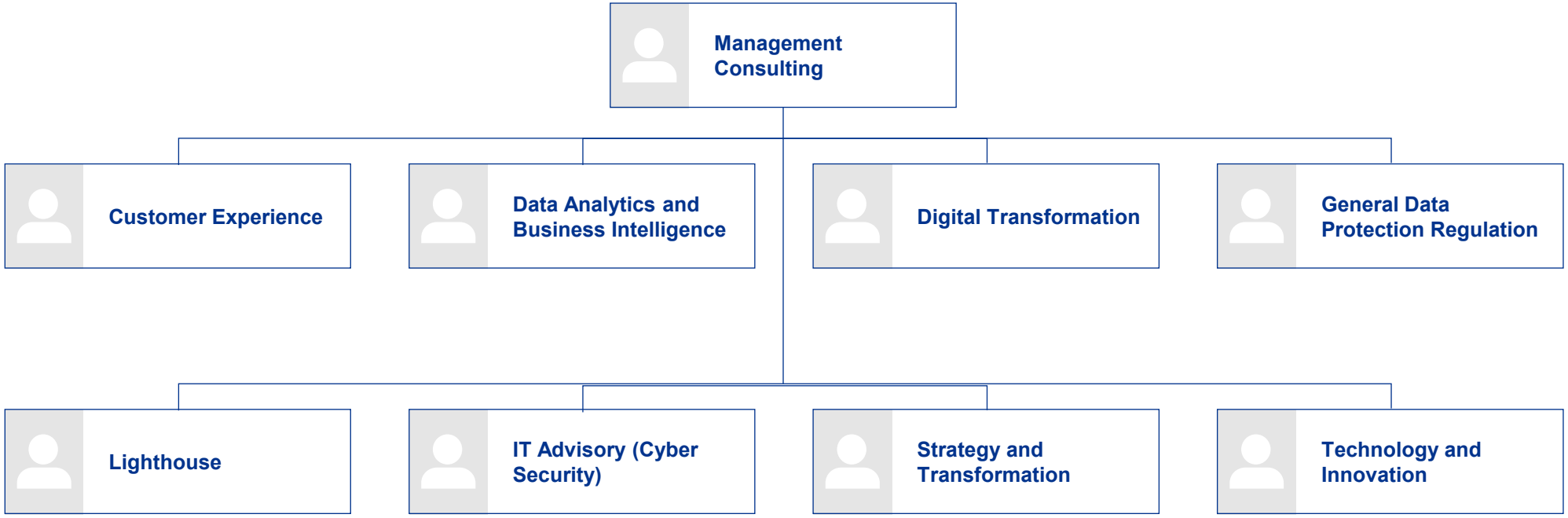
- měsíčník Daňové a právní aktuality (www.danovky.cz)
- Marwick - časopis pro klienty a příznivce KPMG (www.marwick.cz)
- Investment in the Czech Republic
- Studie a průzkumy z vašeho odvětví

Další brožury a studie jsou k dispozici na www.kpmg.cz

Pravidelně pořádáme semináře
a konference s nejrůznějšími oborovým zaměřením
i neformální setkání. Mezi nejvýznamnější patří:

- Daňové a právní fórum v Praze, Olomouci a Českých Budějovicích
- Transfer Pricing Forum
- Finance Forum
- Retail Forum

Organizační schéma (MC)



Cyber Security cluster

01

Soulad s právními předpisy

Audit procesů a organizační struktury v souladu s právními předpisy.

02

Posouzení kybernetické bezpečnosti

Posouzení kybernetické bezpečnosti celé organizace včetně všech typů aktiv.

03

Návrh bezpečné architektury / infrastruktury

Navrhování aplikací, služeb a sítí podle osvědčených postupů v této oblasti.

04

Penetrační testování

Penetrační testování aplikací, webových aplikací, cloudových řešení, mobilních zařízení, sítí atd.

02

Kryptografie - proč by nás měla zajímat?

Na počátku bylo slovo a to slovo bylo tajné.

Všichni máme tajemství. Věci, které nechceme, aby ostatní věděli. Věci, které nechceme sdílet. Je to přirozené. Dalo by se dokonce říci, že je to lidské. Od té doby, co jsme vynalezli komunikaci, jsme také začali vymýšlet metody, jak skrýt její obsah před nežádoucími zvědavci.

Pokud nemáte co skrývat, proč to skrývat?

- Klasický argument proti utajení
- Skutečné soukromí je velmi nový koncept
- Jsou věci, které opravdu potřebujeme skrývat?

Proč by všichni měli znát můj podnik?

- Komu můžeme věřit?
- Může někdo zlomyslně zneužít informace?
- Je život bez tajemství opravdu lepší?
- Panoptikum

Nezbytnost kryptografie v dnešní době

Bez ohledu na to, jaký je váš názor na tuto otázku, je utajení v každodenním životě v moderní práci klíčové.

Metody ověřování pro vládní portály

- hesla
- kryptografické klíče (identita občana).

Šifrovaný webový provoz

- HTTPS
- protokoly pro zajištění pravosti a integrity dat.

Bezpečné platby

- ochrana vašich platebních údajů online
- bezkontaktní platby

Ochrana údajů

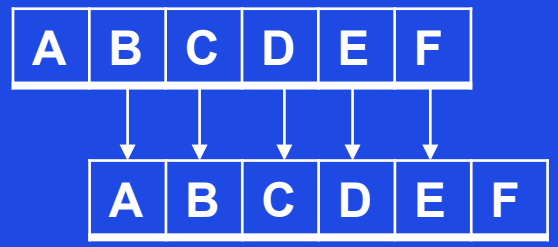
- ochrana přenášených dat před zvědavými pohledy
- šifrování uložených dat, aby se zabránilo jejich poškození v případě úniku.

Slavná (velmi stručná) historie kryptografie

01

Caesarova šifra

- 50 PŘ. N. L.
- Julius Caesar
- Substituční šifra
  - Posun písmen
  - Příklad: posun o 1



02

Enigma

- Počátek 40. let 20. století
- Alan Turing
- Přestože polští matematici přišli na to, jak zprávy Enigmy přečíst, problém spočíval v tom, že se šifra denně měnila.
- Vytvoření dešifrovacího stroje a použití statistické kryptoanalýzy

03

Šifrování veřejným klíčem RSA

- 1977
- MIT
- Algoritmus pro bezpečný přenos dat
- Na základě práce Whitfielda Diffieho a Martina Hellmana
- Spoléhá na modulární aritmetiku a na skutečnost, že
  - Pro libovolná kladná celá čísla e, d, n taková, že 0 <= m <n
  - m^e^d = m mod n
  - m^d^e = m mod n

Cíle kryptografie

Jeden algoritmus se nemůže postarat o všechno! Potřebujeme kombinaci.

Důvěrnost

- Alice pošle zprávu Bobovi, a i když Eva zprávu zachytí, nezíská informace z přenášené zprávy.
- SHA2

Autentičnost

- Když Alice pošle zprávu Bobovi, Bob si může být jistý, že zpráva pochází od Alice a ne od Evy.
- Digitální podpisy

Integrita

- Alice odešle zprávu Bobovi, a pokud Eva zprávu zachytí a upraví, Bob se dozví, že zpráva byla poškozena
- Hash

Neodmítnutí

- Pokud Alice pošle zprávu Bobovi, je jasné, že tak učinila, a nemůže tvrdit, že odesílatelem byla Eva.
- Digitální podpisy / hash

03

Klasická kryptografie

Klíčové pojmy

Obyčejný text

Obyčejné texty jsou jednoduše čitelné zprávy, texty nebo informace.

Šifrový text

Šifrovaný text je transformovaný prostý text tak, aby byl pro člověka nečitelný. Jinými slovy, prostý text po procesu šifrování.

Šifrování

Proces převodu otevřeného textu na šifrovaný text pomocí kryptografické funkce a klíče.

Klíč

Řetězec znaků, který kryptografická funkce používá k zakódování dat tak, aby se jevila jako náhodná.

Dešifrování

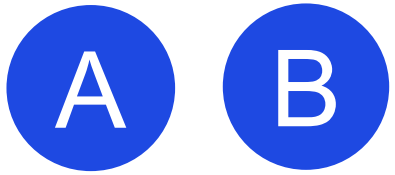
Proces převodu šifrového textu na otevřený text pomocí kryptografické funkce a klíče. (Inverzní funkce k šifrování).

Šifra

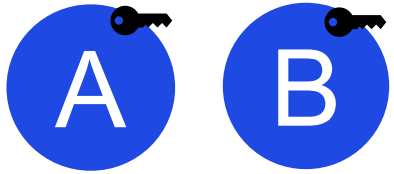
Funkce f(x,k) = y, která využívá 2 vstupy, otevřený text a klíč, k vytvoření šifrového textu.
Existují 2 hlavní typy - bloková a proudová (více o nich později).

Obecný kryptografický algoritmus

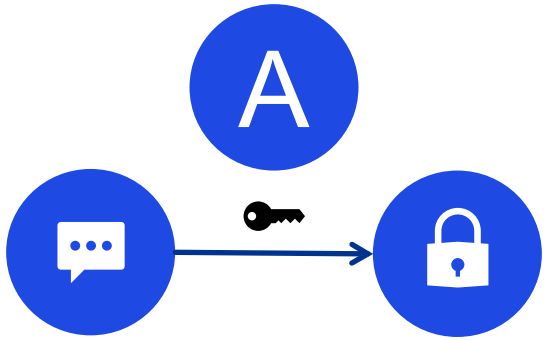
1) Alice chce poslat zabezpečenou zprávu Bobovi.



2) Alice a Bob získají klíče (sdílené tajemství) k šifrování a odšifrování zpráv.

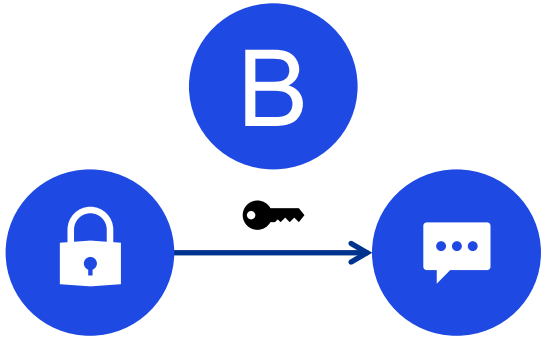


3) Alice použije svůj klíč k zašifrování zprávy s otevřeným textem a změní ji na šifrovaný text.



4) Alice pošle Bobovi zašifrovanou zprávu.

5) Bob použije klíč k odšifrování šifrového textu na otevřený text a může si přečíst zprávu od Alice.

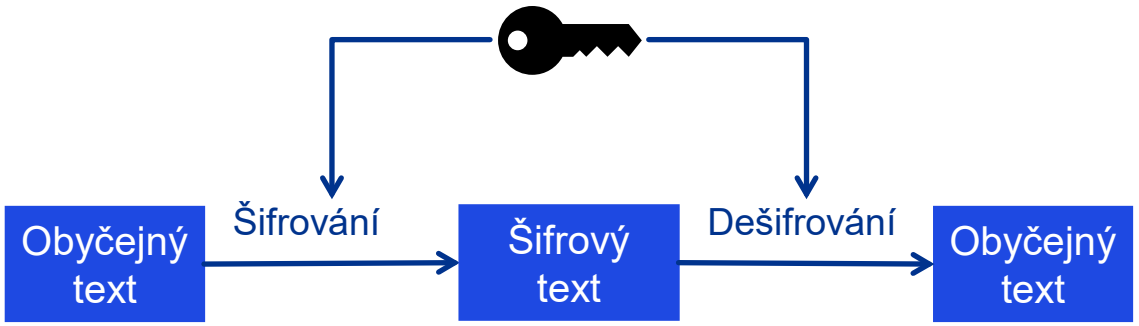


V tomto příkladu se předpokládá bezpečná distribuce klíčů - můžete vymyslet způsob, jak je bezpečně distribuovat sami?

Typy kryptografických algoritmů

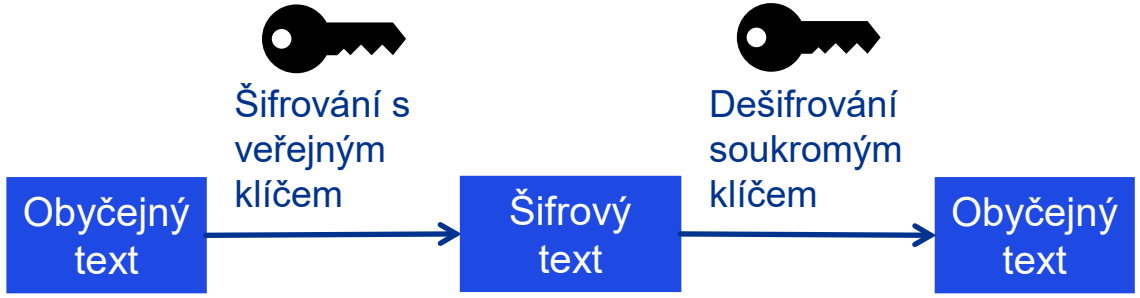
Symetrické

- Pro šifrování a odšifrování se používá stejný klíč.
- Předchozí snímek byl příkladem symetrické kryptografie.
- Rychlejší než asymetrická kryptografie
- AES, RC4, DES, RC5, TC6



Asymetrické

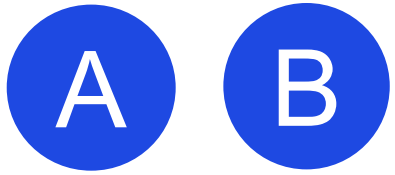
- Nazývá se také kryptografie s veřejným klíčem.
- Pro šifrování a dešifrování se používají různé klíče.
  - Matematicky propojený pár veřejného a soukromého klíče
- Bezpečnější než symetrická kryptografie (vzpomeňte si na problém s distribucí klíčů), ale výpočetně náročnější.
  - Asymetrická kryptografie se poměrně často používá k bezpečnému vytvoření symetrické kryptografie.
- RSA, Diffie-Hellman, ECC



Diffie-Hellman (1/2)

- **Řeší distribuci klíčů**
- **Pro zajištění bezpečnosti jsou nutná mnohem větší čísla než v příkladu.**

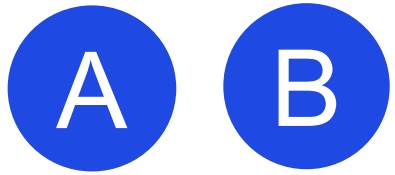
1) Alice a Bob potřebují klíče k bezpečné komunikaci pomocí šifrovaných zpráv.



2) Alice a Bob si zvolí a dohodnou se na p a q tak, že p je prvočíslo a q je generátor p:

p = 11

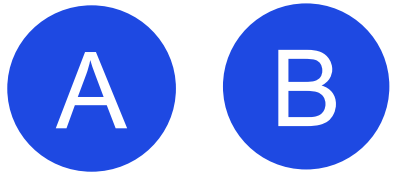
q = 6



3) Alice a Bob si zvolí své osobní klíče a a b (obě čísla jsou prvočísla a jsou menší než p a tajná!):

a = 3

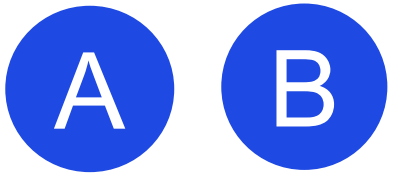
b = 2



4) Alice a Bob vypočítají své veřejné klíče a' a b' tak, že a' = q^a mod p a b' = q^b mod p:

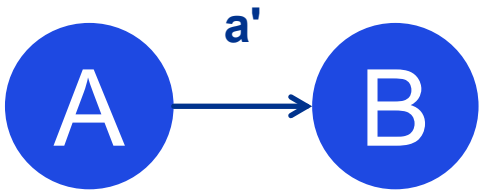
a' = 7

b' = 3

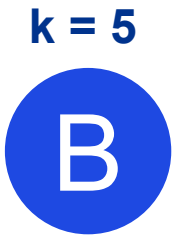


Diffie-Hellman (2/2)

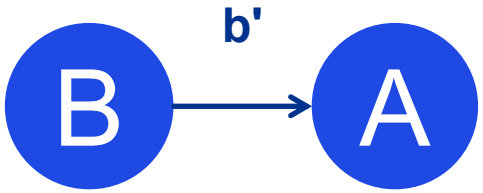
5) Alice sdílí svůj veřejný klíč s Bobem



6) Bob vypočítá tajný klíč pomocí k = a' mod p:



7) Bob sdílí svůj veřejný klíč s Alicí.



6) Alice vypočítá tajný klíč pomocí k = b' mod p:

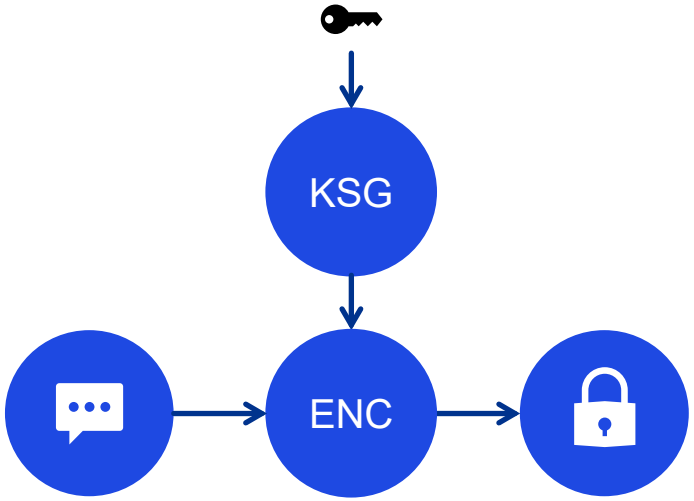
Alice a Bob nyní mohou bezpečně komunikovat pomocí tajného klíče

Hashovací funkce

- **Kryptografické jednosměrné funkce**
- **Mnoho způsobů použití**
  - Kontrolní součty
  - Ochrana hesel
- **Vlastnosti hashovacích funkcí**
  - Deterministické
    - Pro každou f(x1) = y1 a f(x2) = y2 platí, že pokud x1 = x2, pak y1 = y2.
  - Jednosměrný
    - f(x) = y je snadné a rychlé vypočítat, ale je obtížné vypočítat $f^{-1}(y) = x$.
  - Pevná velikost
    - Jakýkoli vstupní text bude mít za následek stejnou pevnou velikost šifrového textu.
  - Lavinový efekt
    - Jakákoli malá změna na vstupu má za následek velkou změnu na výstupu.
  - Odolnost proti kolizi (ideálně)
    - Neexistují x1 a x2 tak, aby x1 != x2 a f(x1) = f(x2)
  - Odolnost proti nalezení druhého vzoru (v praxi)
    - Při zadání vstupu x1 je obtížné najít druhý vstup x2 tak, aby f(x1) = f(x2).
- **Příklady**
  - MD5
  - SHA-1, SHA-2, SHA-3
  - Whirlpool
  - BLAKE2, BLAKE3
  - RIPEMD-160

Proudová šifra

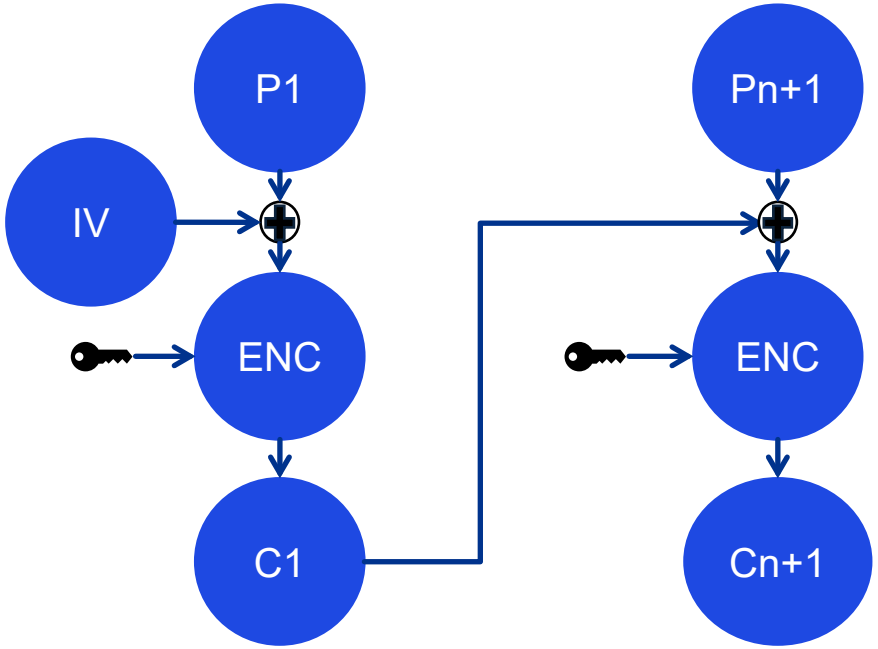
- **nepřetržitě šifruje otevřený text**
- **Rychlejší než bloková šifra (šifruje bit po bitu)**
- **Klíč musí být dlouhý, aby byla kryptoanalýza obtížná.**
- **Čím delší klíč, tím silnější zabezpečení**
- **Pokud klíč není stejně dlouhý jako otevřený text, je znovu použit generátorem proudu klíčů.**
- **Příklad:**
  - Obyčejný text: 0101010101
  - Klíč: 1010101010
  - Šifrový text: 11111111



Bloková šifra

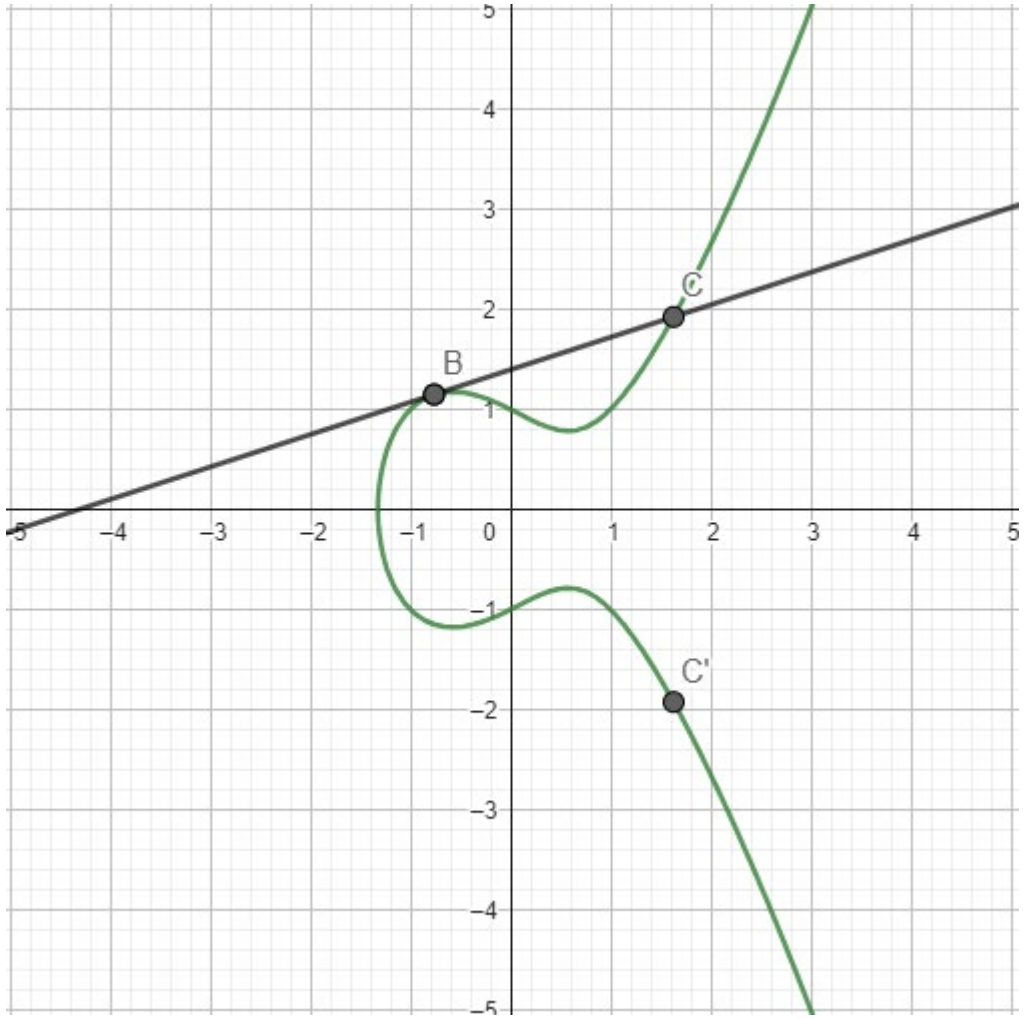
- **Otevřený text je zašifrován po částech o pevné velikosti, které se nazývají bloky.**
- **Režimy provozu** (řetězení bloků)
  - ECB (Electronic Code Book)
  - CBC (Cipher Block Chaining)
  - CFB (Cipher Feedback Mode)
  - OFB (Output Feedback Mode)
- Pomalejší a složitější než proudová šifra
- Bezpečnější než proudová šifra

- **Příklad blokové šifry v režimu ECB**
  - IV = počáteční vektor
  - Pn = blok otevřeného textu n
  - Cn = blok šifrového textu n



Eliptické křivky

- **Eliptická křivka je definována kubickou rovnicí ve dvou proměnných.**
  - Definuje se nad polem K a popisuje body v K^2
  - Nad R (reálná čísla) ve tvaru $y^2 = x^3 + ax + b$
    - Musí být nesingulární (diskriminant musí být nenulový).
  - V modulární aritmetice se dvojnásobek čísla na křivce najde pomocí tečny ke křivce a odrazu v ose x (poté se pro libovolné n udělá přímka mezi n-1 a n-2 a odrazí se průsečík s křivkou v ose x).
  - 2B = C'
  - Bod na křivce se stává soukromým číslem pro algoritmus (při zadání výchozího bodu a jiného bodu na křivce je opravdu těžké určit, kolikrát je násobkem původního čísla).

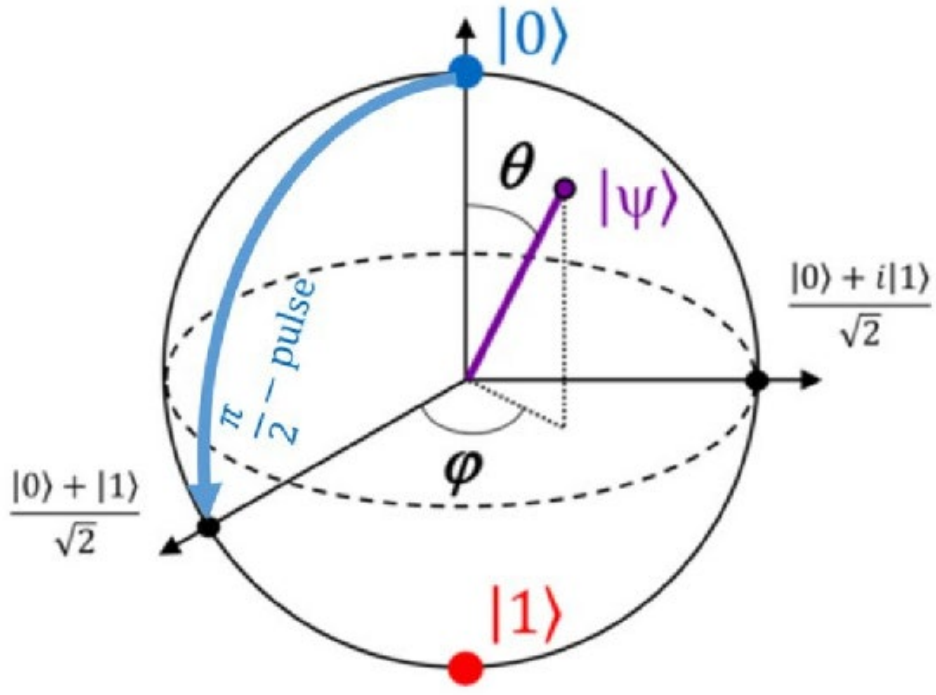


04

Kvantová výpočetní technika

Co je kvantová výpočetní technika?

- **Výpočetní technika využívající kvantově mechanické jevy**
  - Na menších škálách vykazuje fyzikální hmota vlastnosti částic i vln.
- **Qubity místo bitů**
  - Bit je buď 0, nebo 1
  - Qubit se při měření zhroutí na 0 nebo 1, avšak jeho obecný stav může být libovolný díky superpozici.
    - Všechny vypočitatelné stavy současně
    - Blochova sféra



$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$$

Jaký je současný stav?

- **Kvantové výpočty jsou stále velmi experimentální a nepraktické.**
- **Většinou výzkum na univerzitách**
- **Jsou obrovské finanční prostředky na výzkum, protože to je „cool věc“ spolu s AI.**
- **Společnost IBM patří k lídrům**
  - Připravuje 1000 qubitový kvantový čip
  - Stále velmi náchylný k chybám
  - Nyní se zaměřuje na to, aby byl odolnější vůči chybám než na počet qubitů.
  - Vlastní největší kvantový počítač (Osprey) se 433 qubity.
- **Google má menší počítače než IBM, ale ve výzkumu kvantových počítačů je stejně aktivní.**

- **V současné době nemá nikdo rozumnou možnost využívat kvantové výpočty na jiné úrovni než pro výzkum.**
  - Většina algoritmů pro kvantové výpočty je vyvíjena na teoretické úrovni a předpokládá schopnosti, které daleko přesahují náš současný stav.
  - Průlomové objevy z univerzit nebo velkých společností však mohou přijít velmi rychle ve velmi blízké budoucnosti.
- **Omezení na nízké teploty**
  - Čistě kvantový počítač dnes neexistuje.

Kvantová hrozba

- **Global Risk Institute**
  - Roční zpráva o časové ose kvantových hrozeb (Quantum Threat Timeline Report)
  - Panuje široká shoda, že kvantová výpočetní technika se během příštích 30 let stane dostupnou
    - Pravděpodobně ale mnohem dříve
- **Michele Mosca**
  - Institut pro kvantovou výpočetní techniku
  - Michele Mosca Theorem o tom, kdy je třeba jednat:
    - Doba použitelnosti zabezpečení "x
      - Jak dlouho by měla být data v bezpečí
    - Čas migrace "y
      - Jak dlouho trvá zavedení PQC
    - Čas kolapsu (klasické kryptografie) "z
      - Jak dlouho trvá vytvoření dostatečného kvantového počítače
    - Pokud x + y > z, máme problém.

Kvantová hrozba - hlavní rizika pro tradiční kryptografii

S rychlým vývojem kvantové výpočetní techniky představuje kvantová hrozba skutečnost, že většina algoritmů, které byly dříve považovány za bezpečné, je nyní zranitelná a může být kryptoanalyzována. Zejména skrz útok ulož-nyní-odšifruj-později mohou být ohrožena dnes chráněná data vzhledem k jejich životnosti.

Store-Now-Decrypt-Later

- Případ užití protivníka, který shromažďuje data zašifrovaná dnes pomocí kryptografie, která bude zranitelná pomocí kvantových výpočtů.
- To umožní protivníkovi provést kryptoanalýzu uložených dat a způsobit tak odhalení a ztráty u všech cílů, jejichž data zůstávají platná (např. osobní údaje, dlouhodobá hesla).

Paralelní výpočty

- Nové výpočetní paradigma. Nové kvantové výpočetní algoritmy by mohly rozdělit rozsáhlé úlohy hrubé síly na menší úlohy a tyto úlohy pak řešit paralelně.

Ovlivněná kryptografie

- Ovlivňuje současnou technologii veřejných klíčů pro podepisování a výměnu klíčů, včetně algoritmu RSA, algoritmu digitálního podpisu s eliptickou křivkou a algoritmu výměny klíčů Diffie-Hellman.

Kvantová kryptografie

- **Kryptografie využívající kvantovou výpočetní techniku a kvantovou mechaniku.**
  - Kvantová kryptografie nemusí nutně znamenat, že tyto algoritmy jsou kvantově odolné.
  - Velmi zajímavá oblast výzkumu, ale ne tak zásadní jako postkvantová kryptografie.
  - Na základě polarizace fotonů
    - Částice jsou ze své podstaty nejisté
    - Fotony lze měřit náhodně v binárních pozicích
    - Kvantový systém nelze měřit, aniž by byl změněn.
    - Částice lze částečně, ale ne zcela klonovat.

- **Kvantová distribuce klíčů (BB84)**
  - Alice chce poslat soukromý klíč Bobovi
  - Vytvoří dva řetězce **a** a **b** o délce **n**
  - Tyto dva řetězce zakóduje jako tenzorový součin n qubitových stavů.
    - Jeden bit jako data, jeden bit jako klíč k tomu, která báze byla použita.

$$
\begin{aligned}
|\psi_{00}\rangle &= |0\rangle, \\
|\psi_{10}\rangle &= |1\rangle, \\
|\psi_{01}\rangle &= |+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, \\
|\psi_{11}\rangle &= |-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle.
\end{aligned}
$$

  - Odesílá tenzor přes veřejný a ověřený kvantový kanál Bobovi.

Pokračování BB84

- Bob vygeneruje řetězec náhodných bitů **b'** délky b a změří qubity, které obdržel od Alice, čímž vytvoří řetězec **a'.**
- Bob veřejně oznámí, že zprávu obdržel, a Alice veřejně oznámí **b**
- Komunikují spolu veřejným kanálem a zjistí, které bity v **b** a **b'** se shodují, a zbytek Bob i Alice zahodí spolu s odpovídajícími bity v **a a'.**
- Zbývající bity jsou **k**
- Alice si náhodně vybere **k/2** bitů a svou volbu sdělí veřejným kanálem.
- Alice i Bob tyto bity veřejně oznámí a zkontrolují, zda se jich shoduje více než stanovený počet.
  - Pokud kontrola projde, použije se k vytvoření tajných klíčů funkce zesílení soukromí.
  - Pokud kontrola selže, je třeba protokol opakovat
- **Důležité aspekty**
  - Odposlouchávající nemůže mít k dispozici kopii informace.
    - Theorém o nemožnosti klonování
  - Odposlouchávač mohl provádět pouze měření.
    - Na kvantové úrovni měření mění stav!
    - (Alice a Bob to zjistí, protože protokol selže)

05

Postkvantová kryptografie

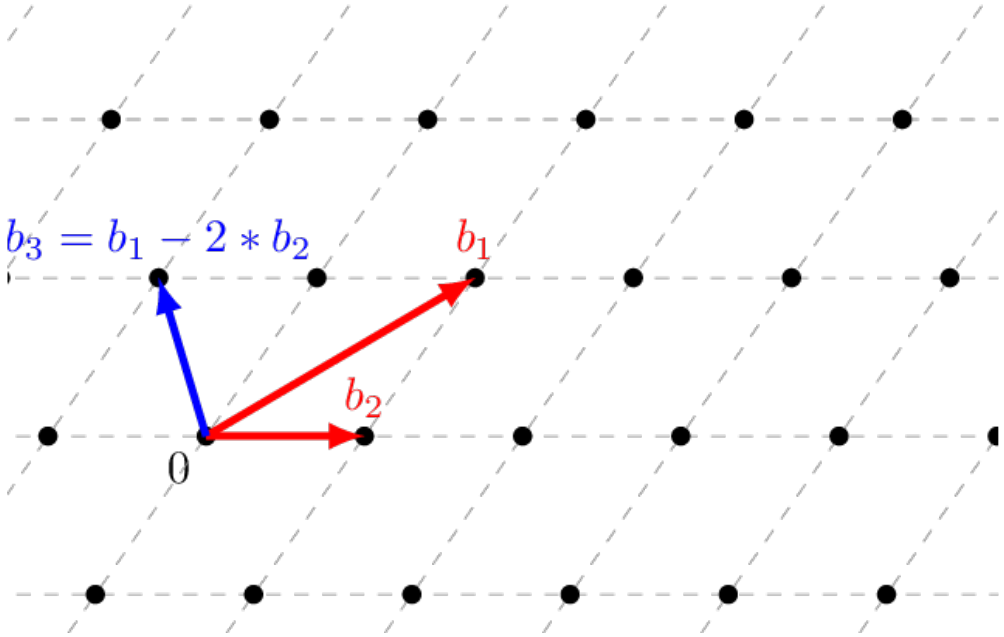
Algoritmy postkvantové kryptografie

- **Postkvantová kryptografie je klasická kryptografie, která je kvantově odolná.**
  - Na základě matematických problémů, které jsou natolik obtížné, že je ani kvantové počítače nedokážou snadno vyřešit.
- **Shorův algoritmus**
  - Kryptografie s veřejným klíčem se opírá o faktorizaci prvočísel, diskrétní logaritmický problém, eliptické křivky.
  - Pokud by bylo možné tyto problémy snadno vyřešit, prolomilo by to kryptografii.
  - V roce 1994 Peter Shor popsal, jak to udělat s kvantovými počítači.
    - Práce na matematickém modelu (idealizovaném)

- **NIST**
  - Národní institut pro standardy a technologie
  - Standardizace postkvantové kryptografie
    - Jsme ve 4. kole podávání žádostí
      - Můžete také přispět tím, že se na ně podíváte a budete je analyzovat / komentovat.
    - Většina algoritmů je založena na mřížce (vybráno pro standardizaci).
      - CRYSTALS
        - Kyber
        - Dilithium
        - CRYSTALS (pq-crystals.org)
    - Zkoumají se další metody
      - kódové, hashové, vícerozměrné, supersingulární založené na isogenii.

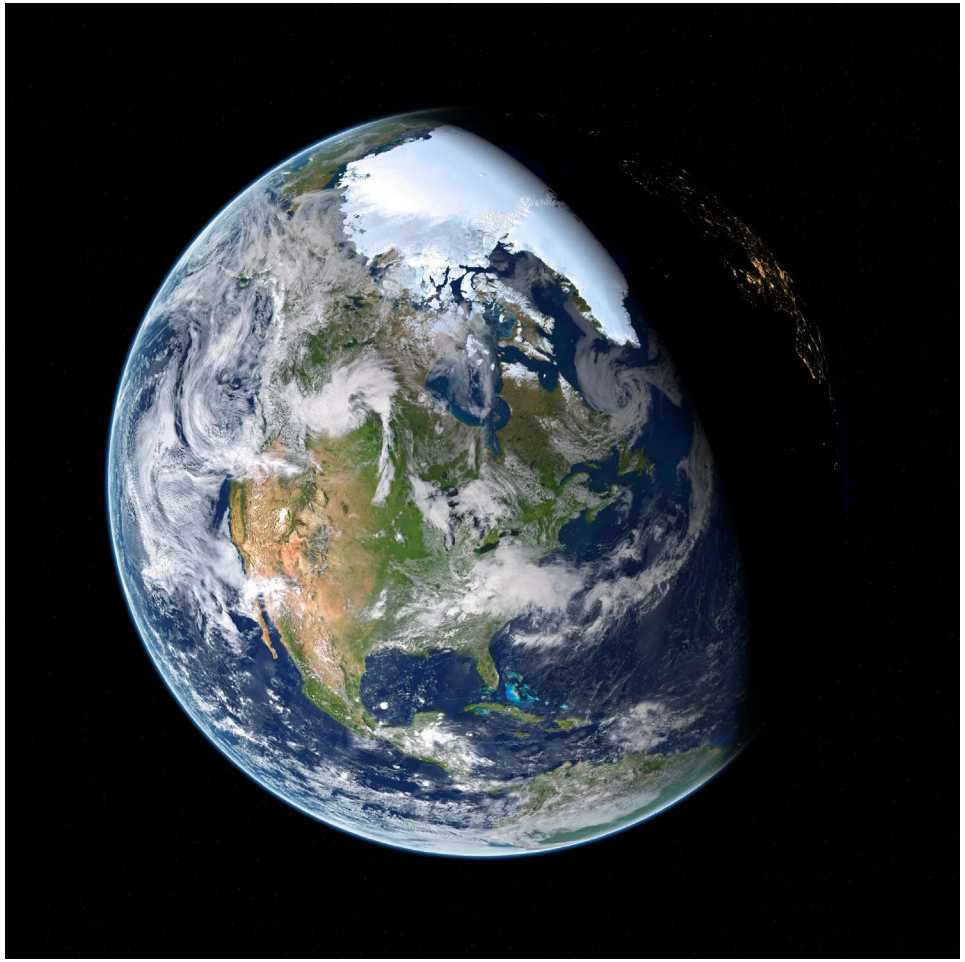
Kryptografie založená na mřížce

- **Mřížka**
  - Opakující se pole bodů (body rozložené podle báze)
- **Základna**
  - Sada základních vektorů, které vytvářejí celou strukturu
  - V příkladu báze = {b1, b2}, protože každý bod v mřížce může být generován jejich lineárními kombinacemi.
  - 2 velmi odlišné sady bázových vektorů mohou generovat stejnou mřížku (věci, které znáte, pokud jste studovali lineární algebru a vektorové prostory).
- **Problém nejkratšího vektoru**
  - Který z bodů mřížky je nejblíže 0 (ale není 0), je-li dán pouze základ.
  - Nyní si představte 3D mřížku, 4D mřížku, 5D mřížku...



Proč bychom měli jednat nyní a nečekat?

- **Pokud budeme čekat, až se kvantová výpočetní technika stane standardem, může být pozdě.**
  - Jakmile se kvantová výpočetní technika stane životaschopnou a Shorův algoritmus bude proveditelný, může veškerá bezpečnost ze dne na den selhat.
  - V cyber security používáme přístup předběžné opatrnosti (riziko nejhoršího scénáře).
- **Překážka pokroku**
  - Pokud budeme čekat, technologie kvantové výpočetní techniky nemusí být záměrně zveřejněna, i když se stane životaschopnou, aby byla chráněna bezpečnost a stabilita výpočetní techniky.
- **Řešení tohoto problému vyžaduje celosvětové úsilí**
  - Celosvětové úsilí je pomalé, zdlouhavé a časově náročné, zejména pokud jde o standardizaci.



Další čtení

- https://www.researchgate.net/figure/Bloch-sphere-Points-on-the-surface-represent-one-qubit-states-ps-Blue-arc-represents-a_fig1_367267169
- https://newsroom.ibm.com/2023-12-04-IBM-Debuts-Next-Generation-Quantum-Processor-IBM-Quantum-System-Two,-Extends-Roadmap-to-Advance-Era-of-Quantum-Utility
- https://www.researchgate.net/figure/Example-of-a-lattice-in-R-2-and-its-basis-b-1-b-2-in-red_fig1_319442001
- The BB84 protocol (Chapter 10) - Quantum Cryptography and Secret-Key Distillation (cambridge.org)
- Migration to Post-Quantum Cryptography | NCCoE (nist.gov)
- Post-Quantum Cryptography | CSRC (nist.gov)
- What Is Quantum-Safe Cryptography? | IBM