Šifrujeme (web)mail

Karel Bílek, česká pirátská strana

Šiřte dle libosti

Drobná odbočka – 2-step autorizace

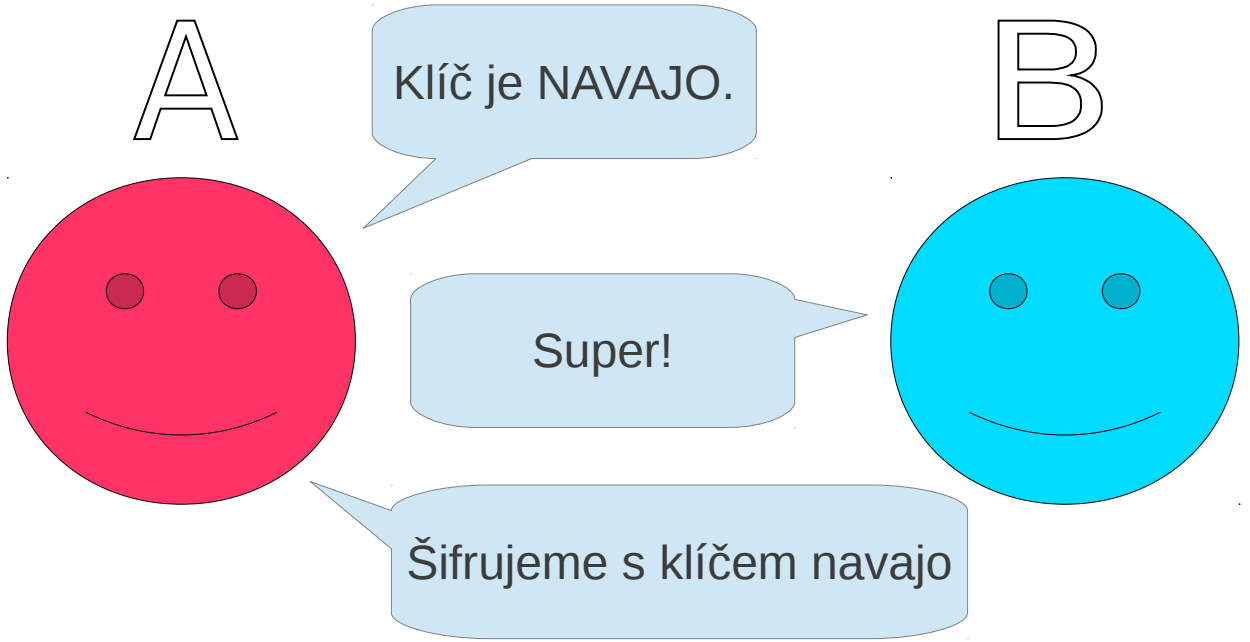
- Používáte GMail?
- Nastavte si 2-factor autorizaci
- Při přihlášení z jiného počítače pošle SMS s kódem
  - Podobně jako např. banka
- Fotka vpravo → account → security → 2-step → start setup
- Česky: účet → zabezpečení → ověření ve 2 krocích → upravit
- Není šifrování, ale zvyšuje bezpečnost

Drobná odbočka – 2-step autorizace

- Bohužel může rozbít 3rd party aplikace
  - Mailové klienty, androidí Gmail aplikaci, pidgin, …
  - Nepřijímají vaše heslo
- Řešení je snadné
  - Fotka → účet → zabezpečení → ověření ve 2 krocích → autorizace aplikací a webů → vytvořit “jednorázové” heslo pro danou aplikaci

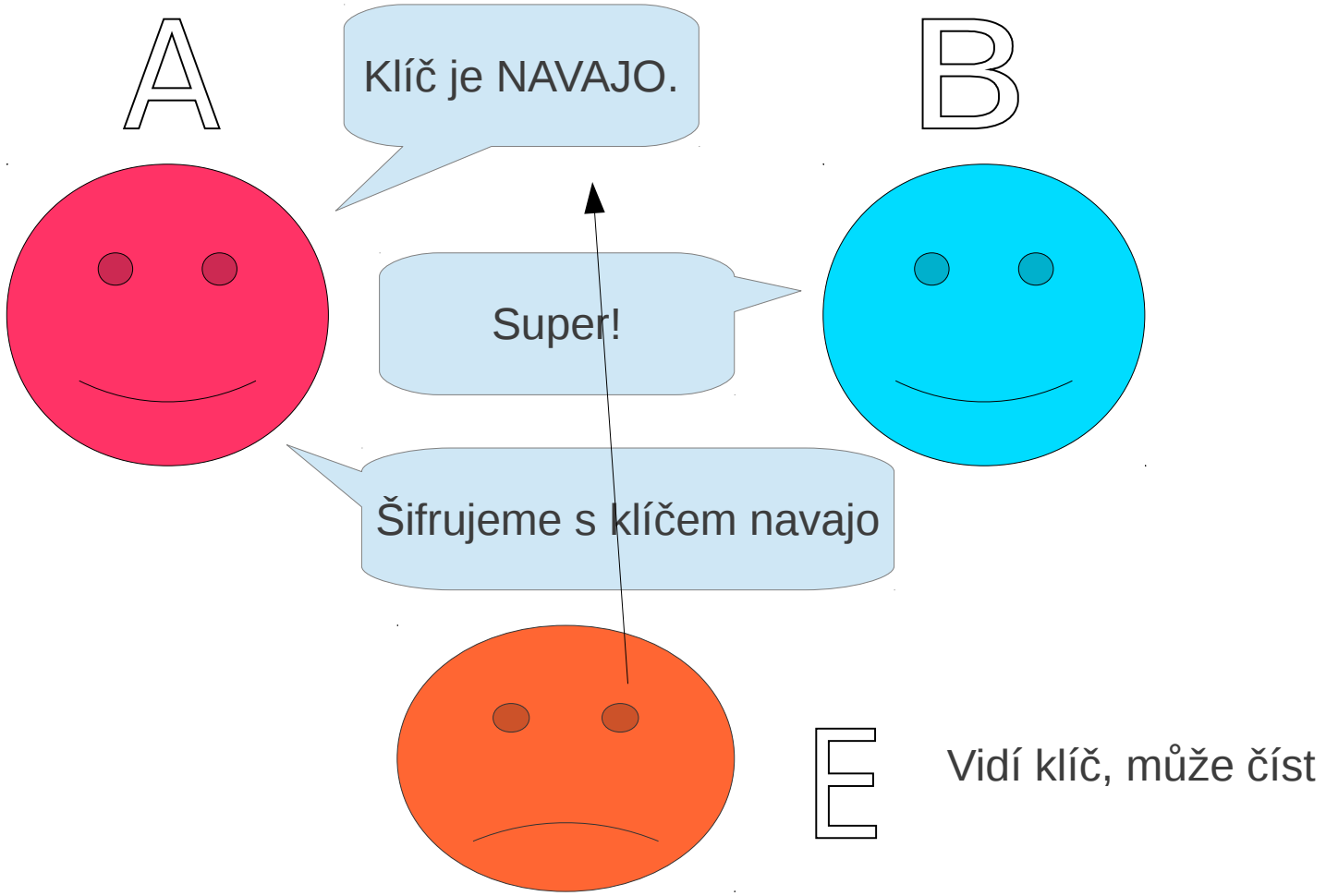
Základy kryptografie s veřejnými klíči

- Klasická kryptografie – oba konce sdílí tajné heslo



Základy kryptografie s veřejnými klíči

- Klasická kryptografie – oba konce sdílí tajné heslo

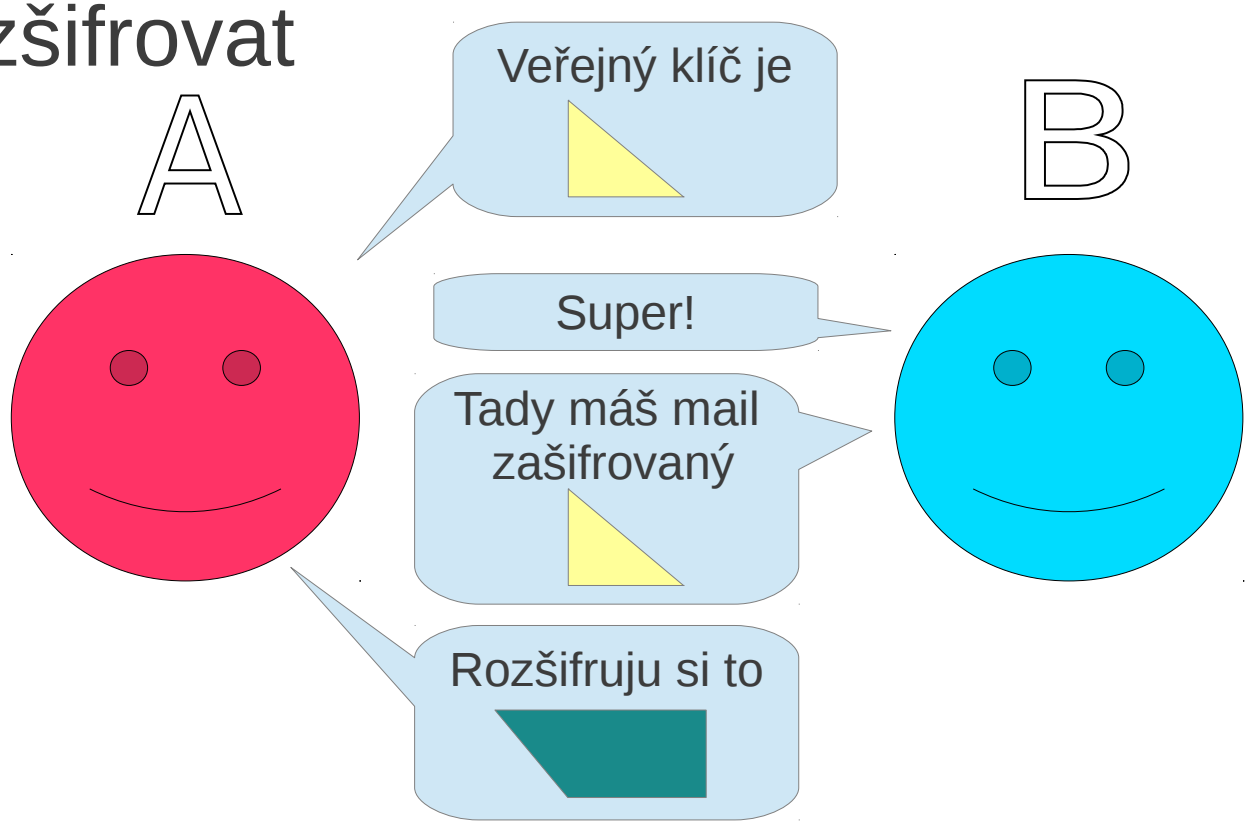


Základy kryptografie s veřejnými klíči

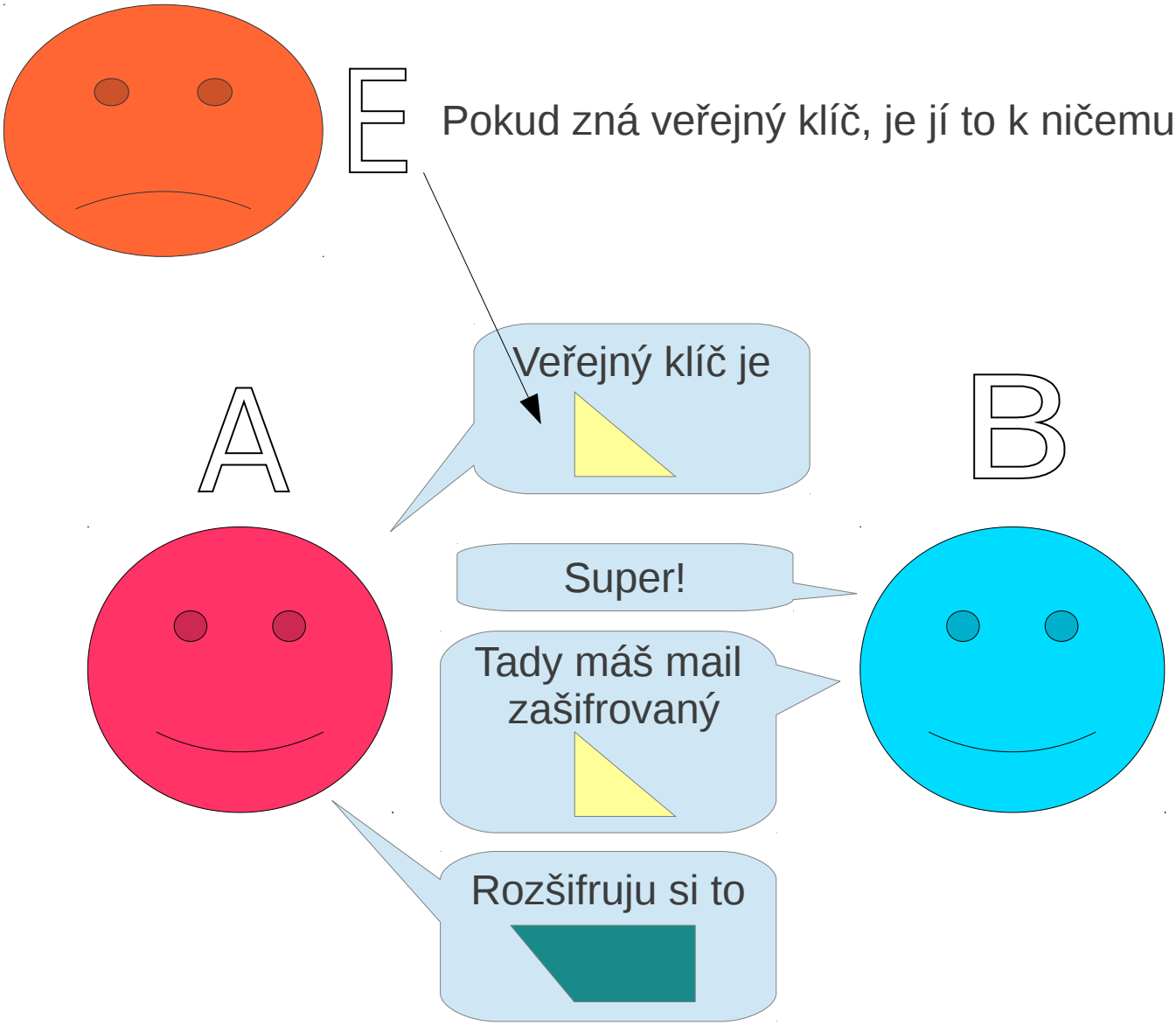
- Public-key kryptografie – klíč má dvě části
- Veřejnou a tajnou část

Základy kryptografie s veřejnými klíči

- Veřejnou část zveřejní **příjemce**
- Můžou vidět všichni
- Pouze příjemce zná **tajnou část** a může rozšifrovat

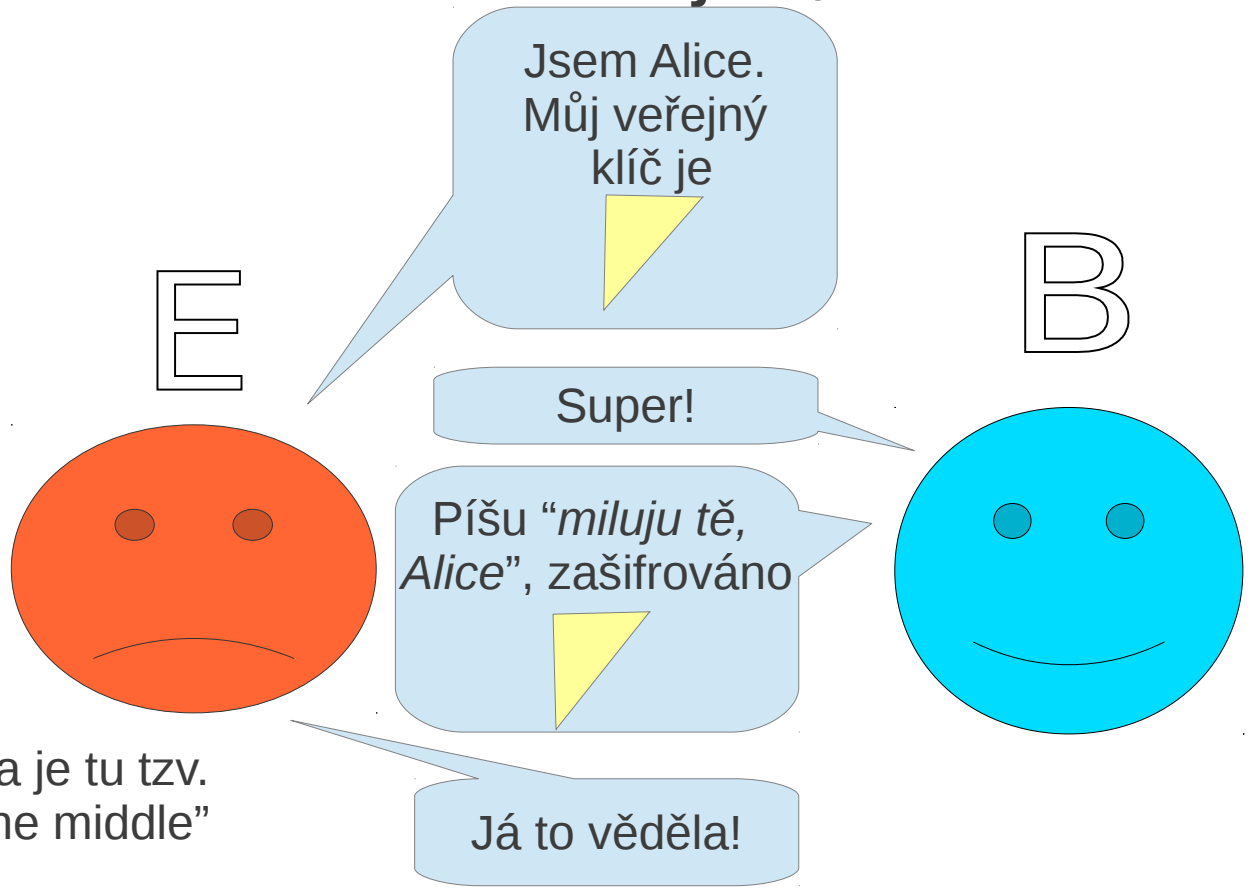


Základy kryptografie s veřejnými klíči



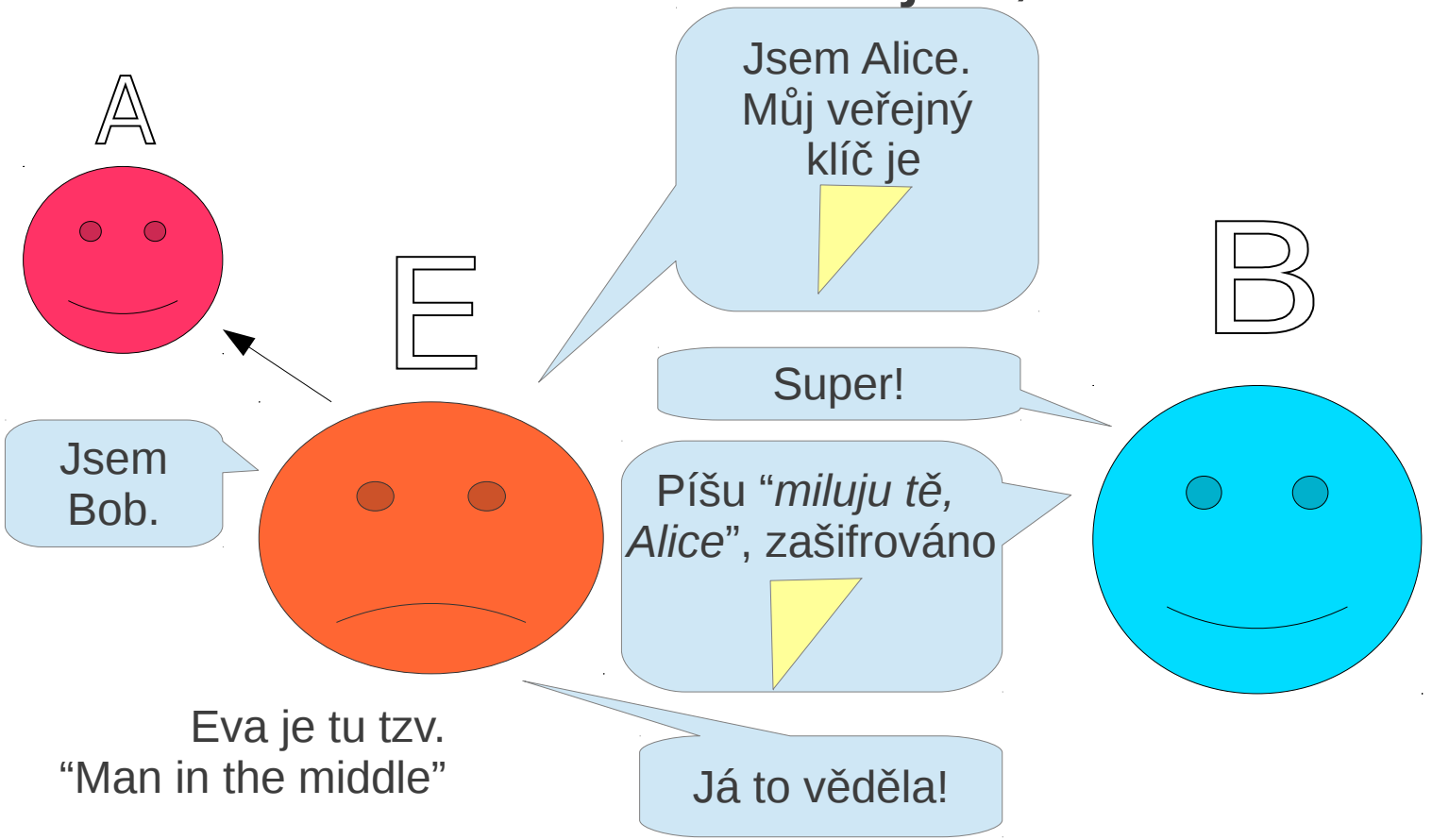
Základy kryptografie s veřejnými klíči

- Je nutné, aby veřejný klíč byl skutečně pravý
- Můžou si ho říct veřejně, ale autentifikovaně

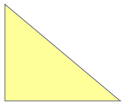
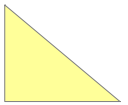
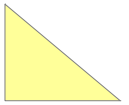


Základy kryptografie s veřejnými klíči

- Je nutné, aby veřejný klíč byl skutečně pravý
- Můžou si ho říct veřejně, ale autentifikovaně



Co teď uděláme?

- Alice si vygeneruje  i 
- Celému světu pošle  , nechá si 
- Bob zašifruje milostné psaní 
- Alice to rozšifruje pomocí 
- Aby Alice mohla odpovědět, musí si svoje klíče vygenerovat i Bob

Co budeme potřebovat?

- Chtěli jsme to ukázat v Thunderbirdu
  - …..ale nikdo s ním neumí a všichni používáme Gmail, resp. seznam
- Dříve neexistovalo šifrování pro webmaily
- Teď existuje!
  - Jmenuje se mailvelope
  - http://ww.mailvelope.com
  - Je to velmi betaverze, nefunguje diakritika
  - I přesto je na šifrování skvělá, protože funguje v browseru (bohužel jen Chrome, FF je alphaverze)

Demo v GMailu