Cyklické grupy a kryptografie

Cyklické grupy, problém výpočtu diskrétního logaritmu

Diffie-Hellmanův protokol na výměnu klíče

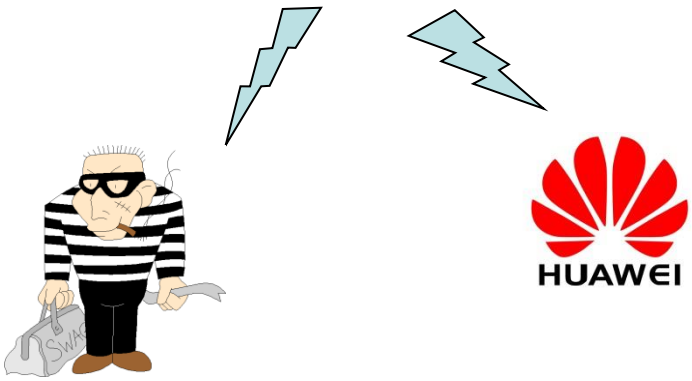
ElGamalův protokol na kryptografii s veřejným klíčem

ElGamalův protokol na digitální podpis

Širší kontext jednosměrných funkcí

Hod mincí, shoda na náhodném bitu

Šifrovaná komunikace: jeden na jednoho



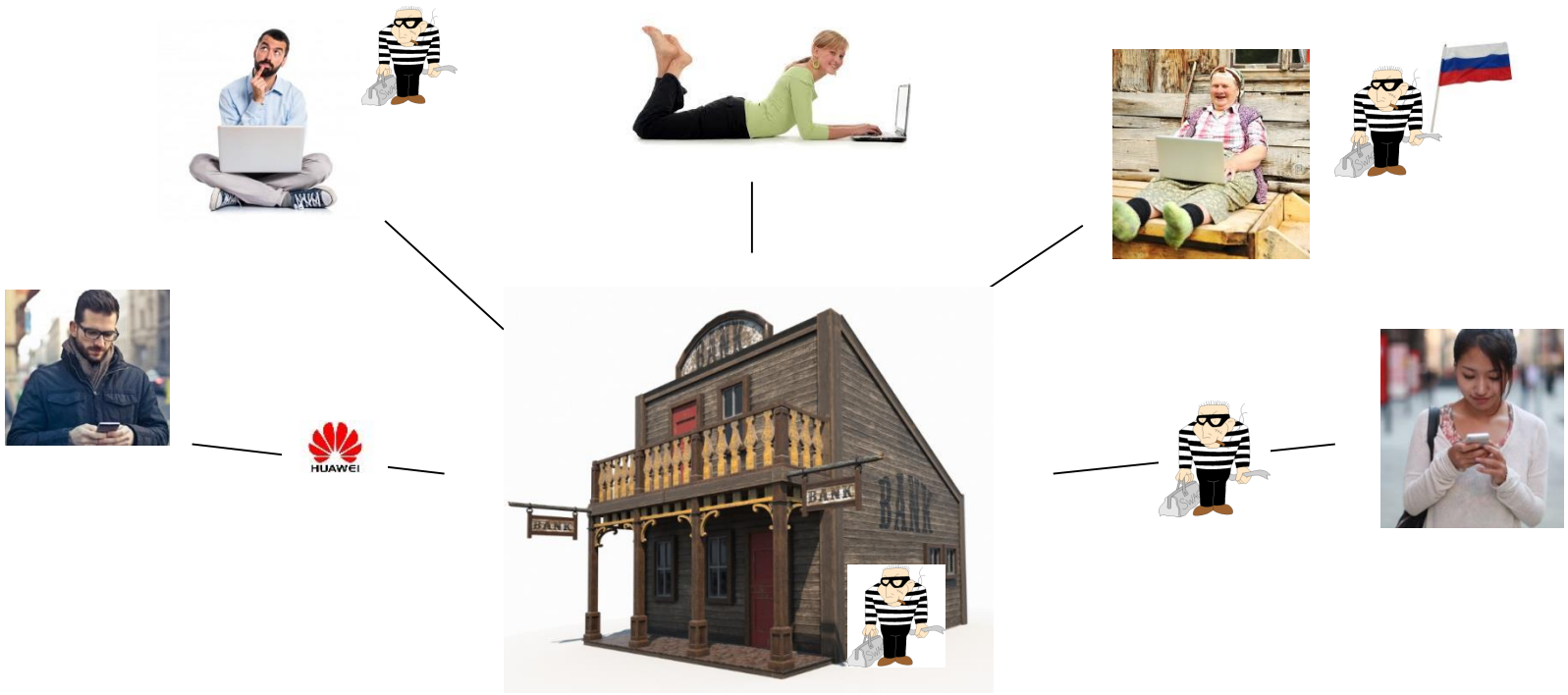
```
KLICJEPODROHOZKOU
HESLOHESLOHESLOHE
----------------
RPANXLTGOFVLGKYVY
```

AES (Advanced Enryption Standard)

Je potřeba se na dálku dohodnout na společném hesle (klíči) !!

→ Diffie-Hellmanův protokol

Šifrovaná komunikace: jeden s mnoha



→ RSA
→ ElGamal

Kryptografie s veřejným klíčem:

- všichni mohou psát pomocí veřejného klíče
- Jen příjemce může číst pomocí tajného klíče

Digitální podpis: potvrzuje identitu odesílatele

- tajný klíč podepisuje, veřejný klíč ověřuje

Cyklické grupy

definice: grupa G je cyklická pokud $\exists a \in G \quad G = \langle a \rangle$

tj. $G = \{a^k : k = 0, \dots, |G|-1\}$ (pro konečné)

Př.: $\mathbb{Z}_n = (\{0, \dots, n-1\}, +\bmod n) = \langle 1 \rangle$

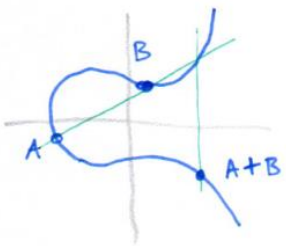
$(n \in \mathbb{N})$ $= \{\underbrace{1+\dots+1}_{k} : k = 0, \dots, n-1\}$

$\mathbb{Z}_p^* = (\{1, \dots, p-1\}, \cdot \bmod p) = \langle a \rangle$ pro jisté a

$(p$ prvočíslo$)$ (není jasné které)

Př.: $E_t(\mathbb{F}_q)$ ... grupy odvozené z eliptických křivek

- obvykle nejsou cyklické
- často obsahují velkou cyklickou podgrupu



Curve25519. Rather concretely, this is the curve $E : y^2 = x^3 + 486662\,x^2 + x$ defined over the field $k = \mathbb{F}_q$, where $q = (2^{255} - 19)^2$ is the square of a prime number. Daniel J. Bernstein et al. [3] showed that the abelian group $E(\mathbb{F}_q)$ has a subgroup $(\mathbb{Z}/n\,\mathbb{Z})$ of order

$$n = 2^{252} + 27742317777372353535851937790883648493$$

as generated by a K-rational point $P = (x_1 : y_1 : 1)$ having coordinate $x_1 = 9$.

Diskrétní exponenciála / logaritmus

$G = \langle a \rangle$ cyklická grupa, $|G| = n$

$\rightsquigarrow$ $\mathbb{Z}_n \rightleftarrows G$ homomorfismy

$k \longmapsto a^k$ ... diskrétní exponenciála

$\log_a b \longleftarrow b$ ... diskrétní logaritmus

👁 v G lze rychle násobit $\Rightarrow$ v G lze rychle mocnit

Idea: $a^{16} = \underbrace{a \cdot a \cdot a \cdot a \cdot \ldots \cdot a}_{16}$ ... POMALU

$= (((a^2)^2)^2)^2$ ... RYCHLE

$a^{21} = a^{2^4} \cdot a^{2^2} \cdot a^{2^0}$ ... využití DVOJKOVÉHO ZÁPISU čísla 21

ALE: není znám žádný obecný algoritmus, který by rychle počítal logaritmus

Př.: $G = \mathbb{Z}_p^*$ kde $p \geq 2^{1000}$

$G = \langle a \rangle \leq \mathbb{E}_t(\mathbb{F}_q)$ kde $q \approx |G| \approx 2^{300}$ (a více)

Diffie-Hellmanův protokol na výměnu klíče

$G = \langle a \rangle$, $|G| = n$



zvol $k \in \{2..n-1\}$

spočti a^k, pošli → x

zvol $\ell \in \{2..n-1\}$

spočti a^ℓ

y ← pošli

spočti y^k

spočti x^ℓ

oba mají stejnou hodnotu $x^\ell = (a^k)^\ell = a^{k\ell} = (a^\ell)^k = y^k$

Co zná nepřítel?

- G, a, $x = a^k$, $y = a^\ell$

Co chce nepřítel? $a^{k\ell}$ ... ALE k, ℓ nezjistí!

ElGamalův protokol

kryptografie s veřejným klíčem

Příjemce zvolí $G = \langle a \rangle$, $|G| = n$

$k \in \{2..n-1\}$ náhodně

$b := a^k$

veřejný klíč: G, a, b

tajný klíč: k

zašifrování: zvol $l \in \{2..n-1\}$ náhodně

$x \mapsto (a^l, x \cdot b^l) \in G \times G$

dešifrování: $(u, v) \mapsto v \cdot u^{-k}$

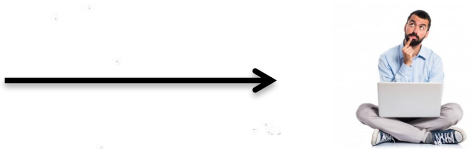
$(a^l, x \cdot b^l) \mapsto x \cdot b^l \cdot (a^l)^{-k} = x \cdot b^l \cdot (a^k)^{-l} = x \cdot b^l \cdot b^{-l} = x$

ElGamalův digitální podpis

$\mathbb{Z}_p^* = \langle a \rangle$, hashovací funkce $H: M \to \mathbb{Z}_{p-1}$

tajný klíč: náhodné $k \in \{2..p-2\}$

veřejný klíč: $b = a^k$ v $\mathbb{Z}_p^*$



podpis: zvol $\ell \in \mathbb{Z}_{p-1}^*$ náhodně (tj. $NSD(p-1, \ell) = 1$)

$\rightsquigarrow \left(\underbrace{a^\ell}_{\text{v grupě } \mathbb{Z}_p^*}, \underbrace{(H(m) - k a^\ell) \cdot \ell^{-1}}_{\text{v okruhu } \mathbb{Z}_{p-1}} \right)$

ověření podpisu: zpráva m, podpis (r, s)

$\rightsquigarrow b^r \cdot r^s \stackrel{?}{=} a^{H(m)}$ v $\mathbb{Z}_p^*$?

... $b^r \cdot r^s = (a^k)^{a^\ell} \cdot (a^\ell)^{(H(m) - k a^\ell)\ell^{-1}} = a^{k \cdot a^\ell} \cdot a^{H(m) - k a^\ell} = a^{H(m)}$

... $x \mapsto a^x$ je bijektivní, čili podepsán musel být hash $H(m)$

ElGamalův digitální podpis

$\mathbb{Z}_p^* = \langle a \rangle$, hashovací funkce $H: M \to \mathbb{Z}_{p-1}$

tajný klíč: náhodné $k \in \{2..p-2\}$

veřejný klíč: $b = a^k$ v $\mathbb{Z}_p^*$

podpis: zvol $\ell \in \mathbb{Z}_{p-1}^*$ náhodně (tj. $NSD(p-1, \ell) = 1$)

$\rightsquigarrow \left(\underbrace{a^\ell}_{\text{v grupě } \mathbb{Z}_p^*}, \underbrace{(H(m) - k a^\ell) \cdot \ell^{-1}}_{\text{v okruhu } \mathbb{Z}_{p-1}} \right)$

ověření podpisu: zpráva m, podpis (r, s)

$\rightsquigarrow b^r \cdot r^s \stackrel{?}{=} a^{H(m)}$ v $\mathbb{Z}_p^*$?

bezpečnost:

- lze zjistit k ? ne, je zamaskované pomocí ℓ^{-1} ... DLOG
- lze vyrobit jinou dvojici podepisující $H(m)$?
  - ↳ bez znalosti k ?

... ℓ lze volit libovolně, čili $r = a^\ell$ lze volit libovolně

chci s t.ž. $b^r \cdot r^s = a^{H(m)}$

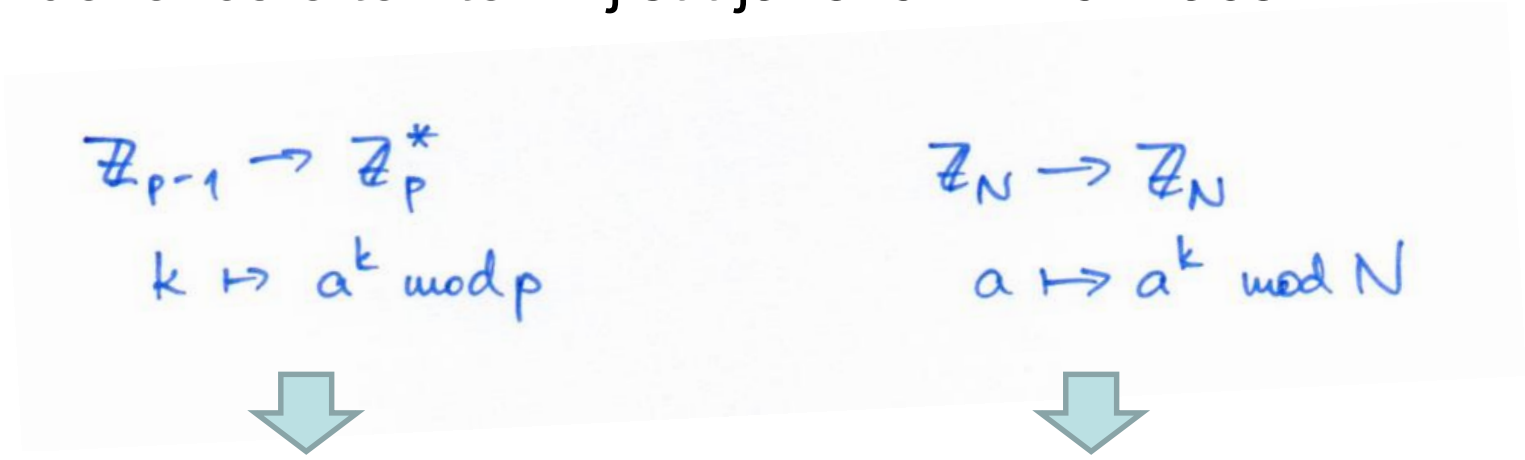
$$r^s = b^{-r} a^{H(m)}$$

$$s = \log_r \left(b^{-r} a^{H(m)} \right) \quad \text{... DLOG}$$

Jednosměrné funkce

zjednodušeně řečeno: funkce *f* taková, že

- hodnotu *f(x)* lze spočítat rychle
- je-li dáno *y*, je obtížné najít *x* takové, že *f(x)=y*, nebo dokonce o tomto *x* zjistit jakékoliv informace



problém diskrétního logaritmu
Diffie-Hellman, ElGamal

(funguje pro *p* prvočíslo)

problém prvočíselného rozkladu
RSA (Rivest, Shamir, Adelman)

(nejbezpečnější pro N=*pq*)

Kámen-nůžky-papír na dálku

A: zahrajem si kámen-nůžky-papír
B: tak jo, raz dva tři teď
A: cos dal ty?
B: nůžky
A: já kámen, vyhrál jsem
B: lžeš
A: hahaha

f: X → Y bijektivní jednosměrná funkce
s: X → {kámen,nůžky,papír} interpretace prvků X jako k-n-p

A: zahrajem si kámen-nůžky-papír
B: tak jo, raz dva tři teď
A: něco jsem dal**, f(x)=38943827520938432908,** cos dal ty?
B: nůžky
A: já kámen, vyhrál jsem
B: lžeš
A: nelžu**, x=54543534530895342985, s(x)=kámen,** ověř si to

→ generování náhodných čísel