Algorithms of Information Security: Kryptografické protokoly

Faculty of Information Technology
Czech Technical University in Prague

October 21, 2020

Lamportův algoritmus jednorázových hesel založený na jednosměrné funkce

- Jádro Lamportova schématu vyžaduje, aby spolupracující komponenty klient/server souhlasily s použitím běžného algoritmu ke generování sady jednorázových hesel (na straně klienta) a ověření klientských hesel obsažených v každém požadavku iniciovaném klientem (na straně serveru).
- Klient generuje konečnou sekvenci hodnot začínajících hodnotou „semínko“ (angl. „seed“) a každá následná hodnota je generována použitím nějakého transformačního algoritmu (nebo funkce $H(w)$) na předchozí hodnotu posloupnosti.

Lamportův algoritmus jednorázových hesel založený na jednosměrné funkce

Příklad konverzace.
Vytvořme pomyslnou konverzaci mezi dvěma lidmi, Alicí a Bobem, kteří zastupují klienta a službu. Předpokládejme, že Alice a Bob sdílejí algoritmus, který byl použit ke generování následující sekvence:

$$18, 21, 24, 27, 40, 44, 47, 50.$$

Naše hodnota semínka (angl. seed) je 18. Funkce $H(w)$ je následující: přidejte 3 a pokud výsledek obsahuje číslici 3, změňte tuto číslici na 4.

Lamportův algoritmus jednorázových hesel založený na jednosměrné funkce

Takto může tato konverzace probíhat:

- Alice: Dobrý den, Bob - chci s vámi mluvit. "Identifier = Alice", "Passkey = 50"
- Bob nemá důvod Alici zamítnout, a tak si uloží záznam komunikace Alice spolu s poskytnutou hodnotou klíče: „Alice“ $\rightarrow$ „50“.
- Alice: Bob, půjčíš mi své auto?: "Identifikátor = Alice", "Passkey = 47"
- Bob se chce ujistit, že je to opravdu Alice. Aplikuje funkci na „47“: $H(47) = 50$. Funkce vrátí „50“: $H(47) = 50$, což odpovídá hodnotě přístupového klíče uloženého v Bobově záznamu. Odpoví Ano a nahradí v záznamu pro Alici: „Alice“ $\rightarrow$ „47“.

- Alice obdrží odpověď a je potěšena, ale uvědomuje si, že neví, kde je Bobovo auto. Nyní žádá, kde je vaše auto?: "Identifikátor = Alice", "Passkey = 44".
- Bob se znovu chce ujistit, že je to opravdu Alice. Stejně jako dříve použije funkci na zadaný klíč: $H(44) = 47$, který odpovídá hodnotě sekvence uložené v záznamu pro Alici. Bob odpoví informacemi, které si Alice vyžádala - roh metra a nádraží - a nahradí v záznamu pro Alici: „Alice“ $\rightarrow$ „44“.
- Alice obdrží informace, které potřebuje, a pak řekne: Díky, Bob! Sbohem: "Identifikátor = Alice", "Passkey = 40".
- Bob si uvědomuje, že Alice je s touto konverzací hotová. Naposledy použije funkci na poskytnutý klíč $H(40) = 44$. Záznam udržovaný pro Alici je nyní vymazán.

One-time passwords based on one-way functions (Lamport's scheme)

- V Lamportově schématu uživatel začíná s tajemstvím w. K definování posloupnosti hesel se používá jednosměrná funkce (OWF), kterou označíme H.
- Posloupnost hesel je následující: $w, H(w), H(H(w)), \ldots, H^t(w)$. Heslo pro i-tou relaci identifikace, kde $1 \leq i \leq t$, je definováno jako $w_i = H^{t-i}(w)$.

Lamportův algoritmus jednorázových hesel založený na jednosměrné funkce

Algorithm 1 Lamportův algoritmus jednorázových hesel založený na jednosměrné funkce

SOUHRN. A se identifikuje B, pomocí jednorázového hesla z posloupnosti hesel

1. *Jednorázové nastavení.*
   - Uživatel A začíná tajemstvím w. Nechť H je jednosměrná funkce.
   - Konstanta t je pevně daná (např.,$t = 100$ nebo 1000), což definuje počet povolených identifikací. (Systém je poté restartován s novým w.)
   - A odešle (*počáteční sdílené tajemství*) $w_0 = H^t(w)$, aby zajistilo svou identifikaci vůči B.
     B inicializuje své počítadlo pro $A : i_A = 1$.

Lamportův algoritmus jednorázových hesel založený na jednosměrné funkce

Algorithm 1 Lamportův algoritmus jednorázových hesel založený na jednosměrné funkce

2. *Zprávy protokolu.* $i-$tá identifikace, $1 \leq i \leq t$, probíhá následovně:

$$A \rightarrow B : A, i, w_i (= H^{t-i}(w)) \qquad (1)$$

$A \rightarrow B : X$ znamená A odešle zprávu X uživateli B.

3. *Akce protokolu.* Aby se A identifikovalo v $i-$té relace, výkoná:
   - A spočte $w_i = H^{t-i}(w)$ (snadno se spočte buď ze samotného w nebo z vhodné mezilehlé hodnoty uložené během výpočtu $H^t(w)$), a pošle (1) B.
   - B ověří, zda $i = i_A$, a zda přijaté heslo w_i splňuje: $H(w_i) = w_{i-1}$. Pokud obě podmínky jsou splněné, B přijme heslo a nastaví $i_A \leftarrow i_A + 1$, a uloží w_i pro další ověření relace.

Lamportův algoritmus jednorázových hesel založený na jednosměrné funkce

Příklad. Předpokládejme, že máme počáteční hodnotu $w = 0$ a chceme vytvořit posloupnost 10 hodnot (kromě počáteční hodnoty), funkce H vypadá následovně:

$$H(w) = w + 3.$$

Aplikujte Lamportův algoritmus (alespoň 2 iterace).

Řešení.

Jednorázové nastavení.

Máme funkci $H(w) = w + 3$ a počáteční hodnotu $w = 0$ a $t = 10$.
Potom posloupnost vypadá takto:

$$0, 3, 6, 9, 12, 15, 18, 21, 24, 27, 30$$

A odešle $B : w_0 = H^t(w)$, což v našem případě je $H^{10}(0) = 30$ a B nastaví čítač pro $A : i_A = 1$.

Jak vypadá zpráva pro první iteraci?

$$A \to B : A, 1, w_1 (= H^9(0) = 27) \qquad (1)$$

Akce protokolu pro první iteraci.

- A spočte $w_1 = H^9(0)$ a pošle B zprávu $A, 1, 27$.
- B ověří, zda $i = i_A$, tedy jestliže $1 = 1$ a ověří jestliže je splněná podmínka: $H(w_1) = w_0$, tj. $H(27) = 27 + 3 = 30$. Obě podmínky jsou splněné, potom B přijme heslo a nastaví $i_A = 2$ a uloží $w_1 = 27$ pro další relace.

Jak vypadá zpráva pro druhou iteraci?

$$A \to B : A, 2, w_2 (= H^8(0) = 24)$$

Akce protokolu pro druhou iteraci.

- A spočte $w_2 = H^8(0) = 24$ a pošle B zprávu $A, 2, 24$.
- B ověří, zda $i_A = 2$ a jestliže je splněná podmínka: $H(w_2) = w_1$, tj. $H(24) = 24 + 3 = 27$. Obě podmínky jsou splněné, potom B přijme heslo a nastaví $i_A = 3$ a uloží $w_2 = 24$ pro další relace.

Stejným způsobem pokračujeme dále.

Feige-Fiat-Shamirův identifikační protokol

- Základní verzi Fiat-Shamirova protokolu lze zobecnit a Feige-Fiat-Shamirův identifikační protokol (FSS) je malou změnou takového zevšeobecnění.
- Protokol FFS zahrnuje identifikaci entity prokazováním znalosti tajemství pomocí důkazu nulové znalosti; protokol neodhaluje žádné částečné informace týkající se tajných identifikačních hodnot A.
- Vyžaduje omezený výpočet (malý zlomek oproti požadavku RSA), a je tedy vhodný pro aplikace s nízkoenergetickými procesory (např., 8bitové čipové karty mikroprocesory).

Feige-Fiat-Shamirův identifikační protokol

Algorithm 2 Feige-Fiat-Shamirův identifikační protokol

SOUHRN. A dokazuje znalost s uživateli B v t iteracích 3-průchodového protokolu.

1. *Výběr parametrů systému.* Důvěryhodné centrum T po výběru dvou tajných prvočísel p a q každé kongruentní s 3 modulo 4 zveřejňuje společný modulus $n = pq$ pro všechny uživatele, a to takový, že n je výpočetně nerealizovatelné faktorizovat. Celá čísla k a t jsou definována jako parametry zabezpečení.

Feige-Fiat-Shamirův identifikační protokol

Algorithm 2 Feige-Fiat-Shamirův identifikační protokol

2. *Výběr tajemství podle jednotlivých entit.* Každá entita A provádí následující.
   - Vybere k náhodných celých čísel $s_1, s_2, \ldots, s_k$ v rozsahu $1 \leq s_i \leq n-1$, a k náhodných bitů $b_1, \ldots, b_k$. (Z technických důvodů je vyžadováno $gcd(s_i, n) = 1$, ale to je téměř jistě zaručeno, protože jinak lze faktorizovat n.)
   - Spočte $v_i = (-1)^{b_i} \cdot (s_i^2)^{-1}$ mod n pro $1 \leq i \leq k$.
   - A se identifikuje nekryptografickými prostředky (např. občankou) T, u které si následně zaregistruje veřejný klíč $A : (v_1, \ldots, v_k; n)$, zatímco pouze A zná svůj soukromý klíč $(s_1, \ldots, s_k)$ a n. Tímto je dokončena jednorázová fáze nastavení.

Feige-Fiat-Shamirův identifikační protokol

Algorithm 2 Feige-Fiat-Shamirův identifikační protokol

3. *Zprávy protokolu.* Každá z t iterací má tři zprávy v následujícím tvaru.

$$A \to B : x \ (= \pm r^2 \bmod n) \tag{1}$$

$$A \leftarrow B : (e_1, \ldots, e_k), e_i \in \{0, 1\} \tag{2}$$

$$A \to B : y \ (= r \cdot \prod_{e_j=1} s_j \bmod n) \tag{3}$$

Feige-Fiat-Shamirův identifikační protokol

Algorithm 2 Feige-Fiat-Shamirův identifikační protokol

4. *Akce protokolu.* Následující kroky jsou provedeny $t$krát; B přijímá identitu A pokud všechny iterace t uspějí. Předpokládejme, že B má autentický veřejný klíč $A : (v_1, \ldots, v_k; n)$; jinak může být certifikát zaslán ve zprávě (1).
   - A vybere náhodné celé číslo $r, 1 \leq r \leq n-1$, a náhodný bit b; vypočítá $x = (-1)^b \cdot r^2 \bmod n$ a pošle x (svědka) B.
   - B pošle A (výzvu), náhodný $k-$bitový vektor $(e_1, \ldots, e_k)$.
   - A vypočítá a odešle B (odpověď) $y = r \cdot \prod_{j=1}^{k} s_j^{e_j} \bmod n$.
   - B spočte $z = y^2 \cdot \prod_{j=1}^{k} v_j^{e_j} \bmod n$, a ověří, že $z = \pm x$ a $z \neq 0$ (to vylučuje úspěch protivníka výběrem $r = 0$).

Příklad. Aplikujte Feige-Fiat-Shamirův identifikační protokol, pokud víme, že důvěryhodné centrum T zvolilo následující tajná prvočísla: $p = 683$ a $q = 811$. Víme, že $k = 3$ a $t = 1$ a předpokládejme, že A vybralo 3 následující náhodná celá čísla: $s_1 = 157, s_2 = 43215$ a $s_3 = 4646$ a 3 náhodné bity $b_1 = 1, b_2 = 0$ a $b_3 = 1$. Dále předpokládejme, že $r = 1279, b = 1$ a víme, že B pošle A následující náhodný vektor $(0, 0, 1)$.

Řešení. Víme, že důvěryhodné centrum T zvolilo následující prvočísla: $p = 683$ a $q = 811$. Nejprve ověříme, jestli prvočísla p a q každé kongruentné 3 modulo 4. Obě prvočísla splňuji danou podmínku. Důvěryhodné centrum T muselo zveřejnit $n = pq = 553913$, přičemž prvočísla p a q důvěryhodné centrum T nezveřejnilo. Dále víme, že $k = 3$ a $t = 1$ a předpokládejme, že A vybralo 3 následující náhodná celá čísla: $s_1 = 157, s_2 = 43215$ a $s_3 = 4646$ a 3 náhodné bity $b_1 = 1, b_2 = 0$ a $b_3 = 1$. Potřebujeme ověřit, jestli $gcd(s_i, n) = 1$, pro $1 \leq i \leq 3$. Danou podmínku splňují s_1, s_2 a s_3.

Spočteme $v_i = (-1)^{b_i} \cdot (s_i^2)^{-1} \bmod n$ pro $1 \leq i \leq 3$.

$$v_1 = (-1)^1 \cdot (157^2)^{-1} = 441845 \bmod 553913$$
$$v_2 = (-1)^0 \cdot (43215^2)^{-1} = 338402 \bmod 553913$$
$$v_3 = (-1)^1 \cdot (4646^2)^{-1} = 124423 \bmod 553913$$

- Veřejný klíč A je $(v_1, v_2, v_3; n)$, tj. $(441845, 338402, 124423; 553913)$
- Soukromý klíč A je (s_1, s_2, s_3) tj. $(157, 43215, 4646)$.

Máme pouze $t = 1$ iteraci, která má tři zprávy v následujícím tvaru.

$$A \to B : x \ (= \pm r^2 \bmod n) \tag{1}$$
$$A \leftarrow B : (e_1, e_2, e_3), e_i \in \{0, 1\} \tag{2}$$
$$A \to B : y \ (= r \cdot \prod_{e_j = 1} s_j \bmod n) \tag{3}$$

- Víme, že A vybralo $r = 1279$ a náhodný bit $b = 1$ dále spočteme $x = (-1)^b \cdot r^2 \bmod n$. Takže $x = (-1)^1 \cdot 1279^2 \bmod 553913$ a pošleme $x = 25898$ uživateli B.
- Předpokládejme, že B pošle A následující náhodný $3-$bitový vektor $(0, 0, 1)$.
- A vypočítá a odešle $B : y = r \cdot \prod_{j=1}^{k} s_j^{e_j} \bmod n$ tj. $y = r \cdot s_3 \bmod n = 403104$.
- B spočte $z = y^2 \cdot v_3 \bmod n = 25898$ a přijme identitu A, jelikož $z = +x$ a $z \neq 0$.

Guillou-Quisquaterův (GQ) identifikační protokol

- Guillou-Quisquaterova (GQ) identifikační schéma je rozšířením Fiat-Shamirova protokolu.
- Guillou-Quisquaterův (GQ) identifikační protokol umožňuje snížení počtu vyměňovaných zpráv a požadavků na paměť pro tajné klíče uživatele a stejně jako Fiat-Shamirův protokol je vhodný pro aplikace, ve kterých má žadatel omezený výkon a paměť.
- Zahrnuje tři zprávy mezi žadatelem A, jehož totožnost má být potvrzena ověřovatelem B.

Guillou-Quisquaterův (GQ) identifikační protokol

Algorithm 3 Guillou-Quisquaterův (GQ) identifikační protokol

SOUHRN. A prokazuje svoji identitu (znalosti s_A) B ve 3 průchodovém protokolu.

1. *Výběr parametrů systému.*
   - Autorita T, které všechny strany důvěřují, pokud jde o vázání identit k veřejným klíčům, vybírá tajné náhodné prvočísla podobně jako v RSA p a q čímž získá modulus $n = pq$.
   - T definuje veřejný exponent $v \geq 3$ s $gcd(v, \phi) = 1$ kde $\phi = (p-1)(q-1)$ a dále spočítá jeho soukromý exponent $s = v^{-1} \bmod \phi$.
   - Systémové parametry (v, n) jsou zpřístupněny (se zaručenou autenticitou) pro všechny uživatele.

Guillou-Quisquaterův (GQ) identifikační protokol

Algorithm 3 Guillou-Quisquaterův (GQ) identifikační protokol

2. *Výběr parametrů podle jednotlivých uživatelů.*
   - Každá entita A má jedinečný identifikátor I_A, ze kterého je odvozena (redundantní identita) $J_A = f(I_A)$, vyhovující $1 < J_A < n$, pomocí známé redundantní funkce f.
   - T dává A tajemství (akreditační údaje) $s_A = (J_A)^{-s} \bmod n$.
3. *Zprávy protokolu.* Každá z t iterací má tři zprávy v následujícím tvaru.

$$A \to B : I_A,\ x = r^v \bmod n \tag{1}$$

$$A \leftarrow B : e \ (\text{kde } 1 \leq e \leq v) \tag{2}$$

$$A \to B : y = r \cdot {s_A}^e \bmod n \tag{3}$$

Guillou-Quisquaterův (GQ) identifikační protokol

Algorithm 3 Guillou-Quisquaterův (GQ) identifikační protokol

4. *Akce protokolu.* A prokazuje svoji identitu B prováděním následujících t iterací; B přijímá identitu pouze v případě, že jsou všechny t provádění úspěšné.
   - A vybírá náhodné tajné celé číslo r (závazek), $1 \leq r \leq n-1$, a počítá (svědka) $x = r^v \bmod n$.
   - A pošle B dvojici celých čísel (I_A, x).
   - B vybere a odešle A náhodné celé číslo e (výzvu), $1 \leq e \leq v$.
   - A vypočítá a odešle B (odpověď) $y = r \cdot {s_A}^e \bmod n$.
   - B přijímá y, konstruuje J_A z I_A pomocí f, spočítá $z = {J_A}^e \cdot y^v \bmod n$, a přijímá důkaz identity od A, pokud obě podmínky jsou splněné $z = x$ a $z \neq 0$ (to vylučuje, aby protivník uspěl s volbou $r = 0$.)

Guillou-Quisquaterův (GQ) identifikační protokol

Příklad. Uvažujme Guillou-Quisquaterův (GQ) identifikační protokol mezi Alicí a Bobem s prvočísly $p = 569, q = 739$ a $v = 54955, t = 1$ a redundantní identita Alice je $J_A = 34579$. Popište komunikaci mezi Alicí a Bobem, pokud ona zvolí $r = 65446$ a on zadá výzvu $e = 38980$.

Guillou-Quisquaterův (GQ) identifikační protokol

Řešení. Podívejme se na Guillou-Quisquaterův (GQ) identifikační protokol s uměle malými parametry a $t = 1$.

1.
   - Nejprve autorita T vybere prvočísla $p = 569$ a $q = 739$ a vypočítá $n = pq = 420491$.
   - Dále T vybere veřejný exponent $v = 54955$ a vypočítá $\phi = (p-1)(q-1) = 419184$. Potom vypočítá jeho soukromý exponent $s = v^{-1} \bmod \phi = 233875$.
   - Systémové parametry jsou (v, n), tj. $(54955, 420491)$, jsou zpřístupněny pro všechny uživatele.

Guillou-Quisquaterův (GQ) identifikační protokol

2.
   - Předpokládejme, že redundantní identita A je $J_A = 34579$.
   - Dále T dává A tajemství (akreditační údaje) $s_A = (J_A)^{-s} \bmod n = 403154$.
3. *Zprávy protokolu.* Každá z t iterací má tři zprávy v následujícím tvaru.

$$A \to B : I_A,\ x = r^v \bmod n \tag{1}$$

$$A \leftarrow B : e \text{ (kde } 1 \leq e \leq v) \tag{2}$$

$$A \to B : y = r \cdot {s_A}^e \bmod n \tag{3}$$

Guillou-Quisquaterův (GQ) identifikační protokol

4.

- A vybere náhodné tajné celé číslo $r = 65446$ a vypočítá $x = r^v \mod n = 89525$.
- A pošle B dvojici celých čísel $(I_A, 89525)$.
- B odešle A náhodné celé číslo (výzvu) $e = 38980$.
- A vypočítá a odešle B (odpověď) $y = r \cdot {s_A}^e \mod n = 83551$.
- B vypočítá $z = {J_A}^e \cdot y^v \mod n = 89525$ a přijímá důkaz identity od A, protože $z = x$.

Schnorrův identifikační protokol

- Schnorrův identifikační protokol je alternativou protokolů Fiat-Shamir a GQ. Jeho bezpečnost je založena na neřešitelnosti problému diskrétního logaritmu.
- Základní myšlenkou je, že A prokazuje znalost tajného a (aniž by jej odhalil) způsobem časově variabilním (v závislosti na výzvě e) a identifikuje se prostřednictvím asociace a s veřejným klíčem v prostřednictvím ověřeného certifikátu A.

Schnorrův identifikační protokol

Algorithm 4 Schnorrův identifikační protokol

SOUHRN. A prokazuje svoji identitu B v 3-průchodovém protokolu.

1. *Výběr parametrů systému.*
   - Vhodné prvočíslo p je vybráno tak, že $p-1$ je dělitelné jiným prvočíslem q. (Najít diskrétní logaritmus modulo p musí být výpočetně neproveditelné, např. $p \approx 2^{1024}, q \geq 2^{160}$.)
   - Prvek β je vybrán tak, že $1 \leq \beta \leq p-1$, má multiplikativní řád q. (Například pro α generátor mod $p, \beta = \alpha^{\frac{(p-1)}{q}} \mod p$.)
   - Každá strana získá autentickou kopii systémových parametrů (p, q, β) a ověřovací funkci (veřejný klíč) důvěryhodné strany T, umožňující ověření podpisů $S_T(m)$ strany T u zpráv m.
   - Je vybrán parametr t (např., $t \geq 40$), $2^t < q$ (definuje úroveň zabezpečení 2^t).

Schnorrův identifikační protokol

Algorithm 4 Schnorrův identifikační protokol

2. *Výběr parametrů podle jednotlivých uživatelů.*
   - Každá entita A má jedinečný identifikátor I_A.
   - A vybere soukromý klíč $a, 0 \leq a \leq q-1$, a spočte $v = \beta^{-a} \bmod p$.
   - A se identifikuje konvenčními prostředky (např. pasem) T, odešle v straně T se zaručenou integritou a získá certifikát $cert_A = (I_A, v, S_T(I_A, v))$ od T, který svazuje I_A s v.
3. *Zprávy protokolu.* Protokol zahrnuje tři zprávy.

$$A \to B : cert_A,\ x = \beta^r \bmod p \tag{1}$$

$$A \leftarrow B : e \text{ (kde } 1 \leq e \leq 2^t < q) \tag{2}$$

$$A \to B : y = ae + r \bmod q \tag{3}$$

Schnorrův identifikační protokol

Algorithm 4 Schnorrův identifikační protokol

4. *Akce protokolu.* A se identifikuje ověřovateli B následujícím způsobem.
   - A vybere náhodné r (závazek), $1 \leq r \leq q-1$, spočte (svědka) $x = \beta^r \bmod p$, a pošle (1) uživateli B.
   - B ověří veřejný klíč v od A tak, že ověří podpis T na $cert_A$, potom pošle A (nikdy předtím použité) náhodné e (výzvu), $1 \leq e \leq 2^t$.
   - A zkontroluje $1 \leq e \leq 2^t$ a odešle B (odpověď) $y = ae + r \bmod q$.
   - B spočte $z = \beta^y v^e \bmod p$, a přijímá identitu A za předpokladu, že $z = x$.

Schnorrův identifikační protokol

Příklad. Uvažujme Schnorrův identifikační protokol mezi Alicí a Bobem s prvočísly $p = 48731$ a $q = 443$, $\alpha = 6$ a $t = 8$ a soukromý klíč Alice je $a = 357$. Popište komunikaci mezi Alicí a Bobem, pokud ona zvolí $r = 274$ a on zadá výzvu $e = 129$.

Schnorrův identifikační protokol

Řešení. Podíváme se na Schnorrův identifikační protokol s uměle malými parametry ze příkladu.

1.
   - Nejprve autorita T vybrala prvočíslo $p = 48731$, kde $p - 1$ je dělitelné jiným prvočíslem $q = 443$.
   - Generátor mod 48731 je $\alpha = 6$ a β je počítán jako $\beta = \alpha^{\frac{(p-1)}{q}} \mod p = 11444$.
   - Systémové parametry jsou (p, q, β), tj. $(48731, 443, 11444)$.
   - Zvolíme $t = 8$.

Schnorrův identifikační protokol

2. • A vybere soukromý klíč $a = 357$ a spočte $v = \beta^{-a} \bmod p = 7355$.
3. *Zprávy protokolu.* Protokol zahrnuje tři zprávy.

$$A \to B : cert_A,\ x = \beta^r \bmod p \tag{1}$$
$$A \leftarrow B : e\ (\text{kde } 1 \leq e \leq 2^t < q) \tag{2}$$
$$A \to B : y = ae + r \bmod q \tag{3}$$

Schnorrův identifikační protokol

4.

- A vybere náhodné $r = 274$ a spočte $x = \beta^r \bmod p = 37123$ a pošle uživateli B.
- B pošle A a náhodnou výzvu $e = 129$.
- A odešle B (odpověď) $y = ae + r \bmod q = 255$.
- B spočte $z = \beta^y v^e \bmod p = 37123$ a přijímá identitu A za předpokladu, že $z = x$.

Schnorrův identifikační protokol

Příklad. Uvažujme Schnorrův identifikační protokol mezi Alicí a Bobem s prvočísly $p = 595939$ a $q = 2027$, $\alpha = 216$ a $t = 8$ a soukromý klíč Alice je $a = 131$. Popište komunikaci mezi Alicí a Bobem, pokud ona zvolí $r = 667$ a on zadá výzvu $e = 13$.

Schnorrův identifikační protokol

Řešení. Podíváme se na Schnorrův identifikační protokol s uměle malými parametry ze příkladu.

1.
   - Nejprve autorita T vybrala prvočíslo $p = 595939$, kde $p - 1$ je dělitelné jiným prvočíslem $q = 2027$.
   - Generátor mod 48731 je $\alpha = 216$ a β je počítán jako $\beta = \alpha^{\frac{(p-1)}{q}} \mod p = 487160$.
   - Systémové parametry jsou (p, q, β), tj. $(595939, 2027, 487160)$.
   - Zvolíme $t = 8$.

Schnorrův identifikační protokol

2. - A vybere soukromý klíč $a = 131$ a spočte $v = \beta^{-a} \bmod p = 477303$.
3. *Zprávy protokolu.*Protokol zahrnuje tři zprávy.

$$A \to B : cert_A,\ x = \beta^r \bmod p \tag{1}$$

$$A \leftarrow B : e\ (\text{ kde } 1 \leq e \leq 2^t < q) \tag{2}$$

$$A \to B : y = ae + r \bmod q \tag{3}$$

Schnorrův identifikační protokol

4.

- A vybere náhodné $r = 667$ a spočte $x = \beta^r \bmod p = 568187$ a pošleuživateli B.
- B pošle A a náhodnou výzvu $e = 13$.
- A odešle B (odpověď) $y = ae + r \bmod q = 343$.
- B spočte $z = \beta^y v^e \bmod p = 568187$ a přijímá identitu A, protože $z = x$.