Matematika IV – Demonstrované cvičení 6
Šifrování

Michal Bulant

Masarykova univerzita
Fakulta informatiky

23. 3. 2009

Obsah přednášky

Doporučené zdroje

- Menezes, Oorschot, Vanstone – *Handbook of Applied Cryptography*, CRC Press, 1996 (též na `http://www.cacr.math.uwaterloo.ca/hac`).

RSA

Ron Rivest, Adi Shamir, Leonard Adleman (1977; C. Cocks,GCHQ – 1973)

- každý účastník A potřebuje dvojici klíčů – veřejný V_A a soukromý S_A

RSA

Ron Rivest, Adi Shamir, Leonard Adleman (1977; C. Cocks,GCHQ – 1973)

- každý účastník A potřebuje dvojici klíčů – veřejný V_A a soukromý S_A
- generování klíčů: zvolí dvě velká prvočísla p, q, vypočte $n = pq$, $\varphi(n) = (p-1)(q-1)$ [n je veřejné, ale $\varphi(n)$ nelze snadno spočítat]

RSA

Ron Rivest, Adi Shamir, Leonard Adleman (1977; C. Cocks,GCHQ – 1973)

- každý účastník A potřebuje dvojici klíčů – veřejný V_A a soukromý S_A
- generování klíčů: zvolí dvě velká prvočísla p, q, vypočte $n = pq$, $\varphi(n) = (p-1)(q-1)$ [n je veřejné, ale $\varphi(n)$ nelze snadno spočítat]
- zvolí **veřejný klíč** e a ověří, že $(e, \varphi(n)) = 1$

RSA

Ron Rivest, Adi Shamir, Leonard Adleman (1977; C. Cocks,GCHQ – 1973)

- každý účastník A potřebuje dvojici klíčů – veřejný V_A a soukromý S_A
- generování klíčů: zvolí dvě velká prvočísla p, q, vypočte $n = pq$, $\varphi(n) = (p-1)(q-1)$ [n je veřejné, ale $\varphi(n)$ nelze snadno spočítat]
- zvolí **veřejný klíč** e a ověří, že $(e, \varphi(n)) = 1$
- např. pomocí Euklidova algoritmu spočítá **tajný klíč** d tak, aby $e \cdot d \equiv 1 \pmod{\varphi(n)}$

RSA

Ron Rivest, Adi Shamir, Leonard Adleman (1977; C. Cocks,GCHQ – 1973)

- každý účastník A potřebuje dvojici klíčů – veřejný V_A a soukromý S_A
- generování klíčů: zvolí dvě velká prvočísla p, q, vypočte $n = pq$, $\varphi(n) = (p-1)(q-1)$ [n je veřejné, ale $\varphi(n)$ nelze snadno spočítat]
- zvolí **veřejný klíč** e a ověří, že $(e, \varphi(n)) = 1$
- např. pomocí Euklidova algoritmu spočítá **tajný klíč** d tak, aby $e \cdot d \equiv 1 \pmod{\varphi(n)}$
- zašifrování numerického *kódu* zprávy M: $C = C_e(M) \equiv M^e \pmod{n}$

RSA

Ron Rivest, Adi Shamir, Leonard Adleman (1977; C. Cocks,GCHQ – 1973)

- každý účastník A potřebuje dvojici klíčů – veřejný V_A a soukromý S_A
- generování klíčů: zvolí dvě velká prvočísla p, q, vypočte $n = pq$, $\varphi(n) = (p-1)(q-1)$ [n je veřejné, ale $\varphi(n)$ nelze snadno spočítat]
- zvolí **veřejný klíč** e a ověří, že $(e, \varphi(n)) = 1$
- např. pomocí Euklidova algoritmu spočítá **tajný klíč** d tak, aby $e \cdot d \equiv 1 \pmod{\varphi(n)}$
- zašifrování numerického *kódu* zprávy M: $C = C_e(M) \equiv M^e \pmod{n}$
- dešifrování šifry C: $OT = D_d(C) \equiv C^d \pmod{n}$

RSA

Ron Rivest, Adi Shamir, Leonard Adleman (1977; C. Cocks,GCHQ – 1973)

- každý účastník A potřebuje dvojici klíčů – veřejný V_A a soukromý S_A
- generování klíčů: zvolí dvě velká prvočísla p, q, vypočte $n = pq$, $\varphi(n) = (p-1)(q-1)$ [n je veřejné, ale $\varphi(n)$ nelze snadno spočítat]
- zvolí **veřejný klíč** e a ověří, že $(e, \varphi(n)) = 1$
- např. pomocí Euklidova algoritmu spočítá **tajný klíč** d tak, aby $e \cdot d \equiv 1 \pmod{\varphi(n)}$
- zašifrování numerického *kódu* zprávy M: $C = C_e(M) \equiv M^e \pmod{n}$
- dešifrování šifry C: $OT = D_d(C) \equiv C^d \pmod{n}$

RSA

Ron Rivest, Adi Shamir, Leonard Adleman (1977; C. Cocks,GCHQ – 1973)

- každý účastník A potřebuje dvojici klíčů – veřejný V_A a soukromý S_A
- generování klíčů: zvolí dvě velká prvočísla p, q, vypočte $n = pq$, $\varphi(n) = (p-1)(q-1)$ [n je veřejné, ale $\varphi(n)$ nelze snadno spočítat]
- zvolí **veřejný klíč** e a ověří, že $(e, \varphi(n)) = 1$
- např. pomocí Euklidova algoritmu spočítá **tajný klíč** d tak, aby $e \cdot d \equiv 1 \pmod{\varphi(n)}$
- zašifrování numerického *kódu* zprávy M: $C = C_e(M) \equiv M^e \pmod{n}$
- dešifrování šifry C: $OT = D_d(C) \equiv C^d \pmod{n}$

Důkaz.

Fermatova, resp. Eulerova věta. $\square$

Příklad

Alice si za parametry svého RSA klíče zvolila $p = 23, q = 31, e = 17$. Dopočítejte její soukromý klíč a pomocí modulárního umocňování na druhou (s možným použitím kalkulačky) zašifrujte (a poté dešifrujte) zprávu $m = 12$.

Příklad

Alice si za parametry svého RSA klíče zvolila $p = 23, q = 31, e = 17$. Dopočítejte její soukromý klíč a pomocí modulárního umocňování na druhou (s možným použitím kalkulačky) zašifrujte (a poté dešifrujte) zprávu $m = 12$.

Řešení

$d = 233$, po zašifrování $c = 538$.

Poznámka

Dosud se bohužel nepodařilo dokázat ani to, že faktorizace (rozklad na prvočísla) čísla n je výpočetně neschůdná, ani to, že prolomit RSA nejde (obecně) snadněji než rozkladem modulu n.

Prvním veřejným kryptosystémem, který je prokazatelně bezpečný (je dokázáno, že jeho prolomení je stejně obtížné jako faktorizace), je **Rabinův kryptosystém**, který si uvedeme ve zjednodušené verzi :

- každý účastník A potřebuje dvojici klíčů – veřejný V_A a soukromý S_A

Poznámka

Dosud se bohužel nepodařilo dokázat ani to, že faktorizace (rozklad na prvočísla) čísla n je výpočetně neschůdná, ani to, že prolomit RSA nejde (obecně) snadněji než rozkladem modulu n.

Prvním veřejným kryptosystémem, který je prokazatelně bezpečný (je dokázáno, že jeho prolomení je stejně obtížné jako faktorizace), je **Rabinův kryptosystém**, který si uvedeme ve zjednodušené verzi :

- každý účastník A potřebuje dvojici klíčů – veřejný V_A a soukromý S_A
- generování klíčů: zvolí dvě podobně velká prvočísla $p, q \equiv 3 \pmod 4$, vypočte $n = pq$.

Poznámka

Dosud se bohužel nepodařilo dokázat ani to, že faktorizace (rozklad na prvočísla) čísla n je výpočetně neschůdná, ani to, že prolomit RSA nejde (obecně) snadněji než rozkladem modulu n.

Prvním veřejným kryptosystémem, který je prokazatelně bezpečný (je dokázáno, že jeho prolomení je stejně obtížné jako faktorizace), je **Rabinův kryptosystém**, který si uvedeme ve zjednodušené verzi :

- každý účastník A potřebuje dvojici klíčů – veřejný V_A a soukromý S_A
- generování klíčů: zvolí dvě podobně velká prvočísla $p, q \equiv 3 \pmod 4$, vypočte $n = pq$.
- $V_A = n$, $S_A = (p, q)$

Poznámka

Dosud se bohužel nepodařilo dokázat ani to, že faktorizace (rozklad na prvočísla) čísla n je výpočetně neschůdná, ani to, že prolomit RSA nejde (obecně) snadněji než rozkladem modulu n.

Prvním veřejným kryptosystémem, který je prokazatelně bezpečný (je dokázáno, že jeho prolomení je stejně obtížné jako faktorizace), je **Rabinův kryptosystém**, který si uvedeme ve zjednodušené verzi :

- každý účastník A potřebuje dvojici klíčů – veřejný V_A a soukromý S_A
- generování klíčů: zvolí dvě podobně velká prvočísla $p, q \equiv 3 \pmod 4$, vypočte $n = pq$.
- $V_A = n$, $S_A = (p, q)$
- zašifrování numerického *kódu* zprávy M: $C = C_e(M) \equiv M^2 \pmod n$

Poznámka

Dosud se bohužel nepodařilo dokázat ani to, že faktorizace (rozklad na prvočísla) čísla n je výpočetně neschůdná, ani to, že prolomit RSA nejde (obecně) snadněji než rozkladem modulu n.

Prvním veřejným kryptosystémem, který je prokazatelně bezpečný (je dokázáno, že jeho prolomení je stejně obtížné jako faktorizace), je **Rabinův kryptosystém**, který si uvedeme ve zjednodušené verzi :

- každý účastník A potřebuje dvojici klíčů – veřejný V_A a soukromý S_A
- generování klíčů: zvolí dvě podobně velká prvočísla $p, q \equiv 3 \pmod 4$, vypočte $n = pq$.
- $V_A = n$, $S_A = (p, q)$
- zašifrování numerického *kódu* zprávy M: $C = C_e(M) \equiv M^2 \pmod n$
- dešifrování šifry C: vypočtou se (čtyři) odmocniny z C modulo n a snadno se otestuje, která z nich byla původní zprávou.

Výpočet druhé odmocniny z C modulo $n = pq$, kde $p \equiv q \equiv 3 \pmod 4$

- vypočti a, b tak, že $ap + bq = 1$
- vypočti $r = C^{(p+1)/4} \pmod p$ a $s = C^{(q+1)/4} \pmod q$
- polož $x = (aps + bqr) \pmod n$, $y = (aps - bqr) \pmod n$
- druhými odmocninami z C modulo n jsou $\pm x$, $\pm y$.

Příklad

V Rabinově kryptosystému Alice zvolila za svůj soukromý klíč $p = 23, q = 31$, veřejným klíčem je pak $n = pq = 713$. Zašifrujte zprávu $m = 327$ pro Alici a ukažte, jak bude alice tuto zprávu dešifrovat.

Příklad

V Rabinově kryptosystému Alice zvolila za svůj soukromý klíč $p = 23, q = 31$, veřejným klíčem je pak $n = pq = 713$. Zašifrujte zprávu $m = 327$ pro Alici a ukažte, jak bude alice tuto zprávu dešifrovat.

Řešení

$c = 692$, kandidáti původní zprávy jsou $\pm 4 \cdot 23 \cdot 14 \pm 3 \cdot 31 \cdot 18 \pmod{713}$.

Diffie-Hellman key exchange, ElGamal

Whitfield Diffie, Martin Hellman (1976; M. Williamson, GCHQ - 1974)
Výměna klíčů pro symetrickou kryptografii bez předchozího kontaktu (tj. náhrada jednorázových klíčů, kurýru s kufříky, ...).

Diffie-Hellman key exchange, ElGamal

Whitfield Diffie, Martin Hellman (1976; M. Williamson, GCHQ - 1974)

Výměna klíčů pro symetrickou kryptografii bez předchozího kontaktu (tj. náhrada jednorázových klíčů, kurýru s kufříky, …).

- Dohoda stran na **cyklické grupě** G a jejím generátoru g (veřejné)

Diffie-Hellman key exchange, ElGamal

Whitfield Diffie, Martin Hellman (1976; M. Williamson, GCHQ - 1974)

Výměna klíčů pro symetrickou kryptografii bez předchozího kontaktu (tj. náhrada jednorázových klíčů, kurýru s kufříky, ...).

- Dohoda stran na **cyklické grupě** G a jejím generátoru g (veřejné)
- Alice vybere náhodné a a pošle g^a

Diffie-Hellman key exchange, ElGamal

Whitfield Diffie, Martin Hellman (1976; M. Williamson, GCHQ - 1974)

Výměna klíčů pro symetrickou kryptografii bez předchozího kontaktu (tj. náhrada jednorázových klíčů, kurýru s kufříky, ...).

- Dohoda stran na **cyklické grupě** G a jejím generátoru g (veřejné)
- Alice vybere náhodné a a pošle g^a
- Bob vybere náhodné b a pošle g^b

Diffie-Hellman key exchange, ElGamal

Whitfield Diffie, Martin Hellman (1976; M. Williamson, GCHQ - 1974)

Výměna klíčů pro symetrickou kryptografii bez předchozího kontaktu (tj. náhrada jednorázových klíčů, kurýru s kufříky, ...).

- Dohoda stran na **cyklické grupě** G a jejím generátoru g (veřejné)
- Alice vybere náhodné a a pošle g^a
- Bob vybere náhodné b a pošle g^b
- Společným klíčem pro komunikaci je g^{ab}.

Diffie-Hellman key exchange, ElGamal

Whitfield Diffie, Martin Hellman (1976; M. Williamson, GCHQ - 1974)

Výměna klíčů pro symetrickou kryptografii bez předchozího kontaktu (tj. náhrada jednorázových klíčů, kurýru s kufříky, ...).

- Dohoda stran na **cyklické grupě** G a jejím generátoru g (veřejné)
- Alice vybere náhodné a a pošle g^a
- Bob vybere náhodné b a pošle g^b
- Společným klíčem pro komunikaci je g^{ab}.

Diffie-Hellman key exchange, ElGamal

Whitfield Diffie, Martin Hellman (1976; M. Williamson, GCHQ - 1974)

Výměna klíčů pro symetrickou kryptografii bez předchozího kontaktu (tj. náhrada jednorázových klíčů, kurýru s kufříky, ...).

- Dohoda stran na **cyklické grupě** G a jejím generátoru g (veřejné)
- Alice vybere náhodné a a pošle g^a
- Bob vybere náhodné b a pošle g^b
- Společným klíčem pro komunikaci je g^{ab}.

Poznámka

- Původní (a nejobvyklejší) volba G je multipliktivní grupa invertibilních zbytkových tříd modulo prvočíslo p, její generátor bývá také nazývám *primitivní kořen modulo p* .
- Problém diskrétního logaritmu (DLP)
- Nezbytná autentizace (*man in the middle attack*)

Příklad

Demonstrujte dohodu Alice a Boba na tajném klíči v DH systému na výměnu klíčů se (všem) známými parametry $G = (\mathbb{Z}_{23}^{\times}, \cdot)$, $g = 5$.

Příklad

Demonstrujte dohodu Alice a Boba na tajném klíči v DH systému na výměnu klíčů se (všem) známými parametry $G = (\mathbb{Z}_{23}^{\times}, \cdot)$, $g = 5$.

Řešení

Možností je mnoho, např. $a = 13, b = 20$, Alice posílá $5^{13} \equiv 21 \pmod{23}$, Bob posílá $5^{20} \equiv 12 \pmod{23}$, pak klíčem je $21^{20} \equiv 12^{13} \equiv 6 \pmod 2)3$.

Z protokolu DH na výměnu klíčů odvozen šifrovací algoritmus ElGamal:

- Alice zvolí cyklickou grupu G spolu s generátorem g
- Alice zvolí **tajný klíč** x, spočítá $h = g^x$ a zveřejní **veřejný klíč** (G, g, h)
- šifrování zprávy M: Bob zvolí náhodné y a vypočte $C_1 = g^y$ a $C_2 = M \cdot h^y$ a pošle (C_1, C_2)
- dešifrování zprávy: $OT = C_2/C_1^x$

Příklad

Alice zvolila za parametry v kryptosystému ElGamal $p = 23, g = 5$, za svůj soukromý klíč zvolila $x = 13$ a zveřejnila veřejný klíč (p, g, g^x). Ukažte, jak Bob zašifruje zprávu $M = 17$ určenou Alici a jak tuto zprávu následně Alice dešifruje.

Příklad

Alice zvolila za parametry v kryptosystému ElGamal $p = 23, g = 5$, za svůj soukromý klíč zvolila $x = 13$ a zveřejnila veřejný klíč (p, g, g^x). Ukažte, jak Bob zašifruje zprávu $M = 17$ určenou Alici a jak tuto zprávu následně Alice dešifruje.

Řešení

Bob zvolí např. $y = 12$, dopočte $C_1 \equiv 5^{12} \equiv 18 \pmod{23}$ a $C_2 = M \cdot (21)^{12} \equiv 11 \pmod{23}$. Alice (díky znalosti x) spočítá $M = C_2 / C_1^x \equiv 17 \pmod{23}$.