Izbrani algoritmi
Deljenje skrivnosti

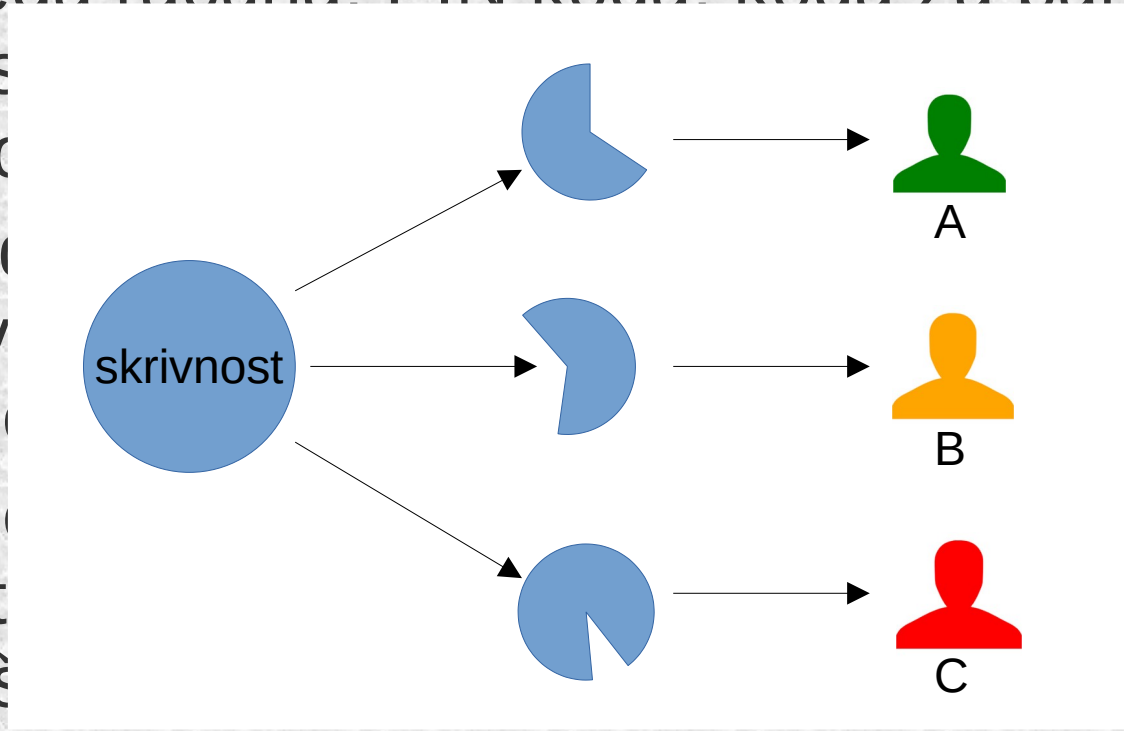
Damjan Strnad

Deljenje skrivnosti

- **skrivnost** (secret) *S* je nek pomemben podatek (št. bančnega računa, PIN koda, koda za bančni trezor ali jedrsko orožje), ki ga želimo hkrati zavarovati pred zlonamerno uporabo in izgubo
  - v nadaljni obravnavi bomo predpostavili, da je skrivnost *S* številska vrednost (v nasprotnem primeru jo vanjo pretvorimo)
- **deljenje skrivnosti** (secret sharing) se nanaša na razdelitev deležev skrivnosti med množico *N* pooblaščenih oseb, tako da je za rekonstrukcijo skrivnosti potrebnih vsaj *K* katerihkoli deležev*
  - takšno shemo imenujemo **(*K*,*N*)-pragovna shema** ((*K*,*N*)-threshold scheme)

Deljenje skrivnosti

- **skrivnost** (secret) *S* je nek pomemben podatek (št. bančnega računa, PIN koda, koda za bančni trezor ali jedrs arovati pred zl
  - v na li, da je skriv otnem prim
- **deljenj** anaša na razdelit o *N* pooblaš rukcijo skrivnosti potrebnih vsaj *K* katerihkoli deležev*
  - takšno shemo imenujemo **(*K*,*N*)-pragovna shema** ((*K*,*N*)-threshold scheme)



(*K*,*N*)-pragovna shema

- razdelitev skrivnosti na deleže in njihovo delitev med *N* zaupnikov izvede zaupen **delivec** (dealer)
  - zaupnikom lahko priredimo različne teže, tako da jim dodelimo različna števila deležev
- zahteva 1: katerakoli podmnožica *K* zaupnikov lahko rekonstruira skrivnost
- zahteva 2: nobena podmnožica *K*-1 zaupnikov ne more pridobiti nobene informacije o skrivnosti

(*K*,*N*)-pragovna shema

- primer uporabe (2,3)-pragovne sheme:
  - kodo za bančni trezor razdelimo na tri deleže, ki jih dobijo trije uslužbenci banke
  - ker se želimo zavarovati za primer pokvarjenega uslužbenca, morata za rekonstrukcijo kode sodelovati vsaj dva uslužbenca
  - ker ne želimo, da bi postal bančni trezor nedostopen zaradi nepričakovane smrti katerega od uslužbencev, sta za rekonstrukcijo kode dva uslužbenca tudi dovolj

(*K*,*N*)-pragovna shema

- zgled za *K*=*N*: (2,2)-pragovna shema
  - skrivnost *S* je binarno število, npr. 100101
  - poskus 1: vsakemu zaupniku damo polovico gesla (npr. 100 in 101) ⇒ zahteva 2 ni izpolnjena
  - poskus 2:
    - delež S_1 prvega zaupnika je naključno binarno število enake dolžine kot *S*, npr. 110100
    - delež S_2 drugega zaupnika je *S* XOR S_1, t.j. 010001
    - zahteva 2 je izpolnjena, saj s poznavanjem S_1 nismo pridobili nobene informacije o *S*
    - enostavno razširljivo na (*N*,*N*) za *N*>2

(*K*,*N*)-pragovna shema

- shemo (*N*,*N*) lahko uporabimo za implementacijo poljubne sheme (*K*,*N*), kjer je 1<*K*<*N*
  - izvedemo $\binom{N}{K}$ delitev na *K* deležev, ki jih razdelimo med vse možne podmnožice *K* upravičencev
  - postopek postane nepraktičen za večje vrednosti *K* in *N*

Shamirjeva metoda

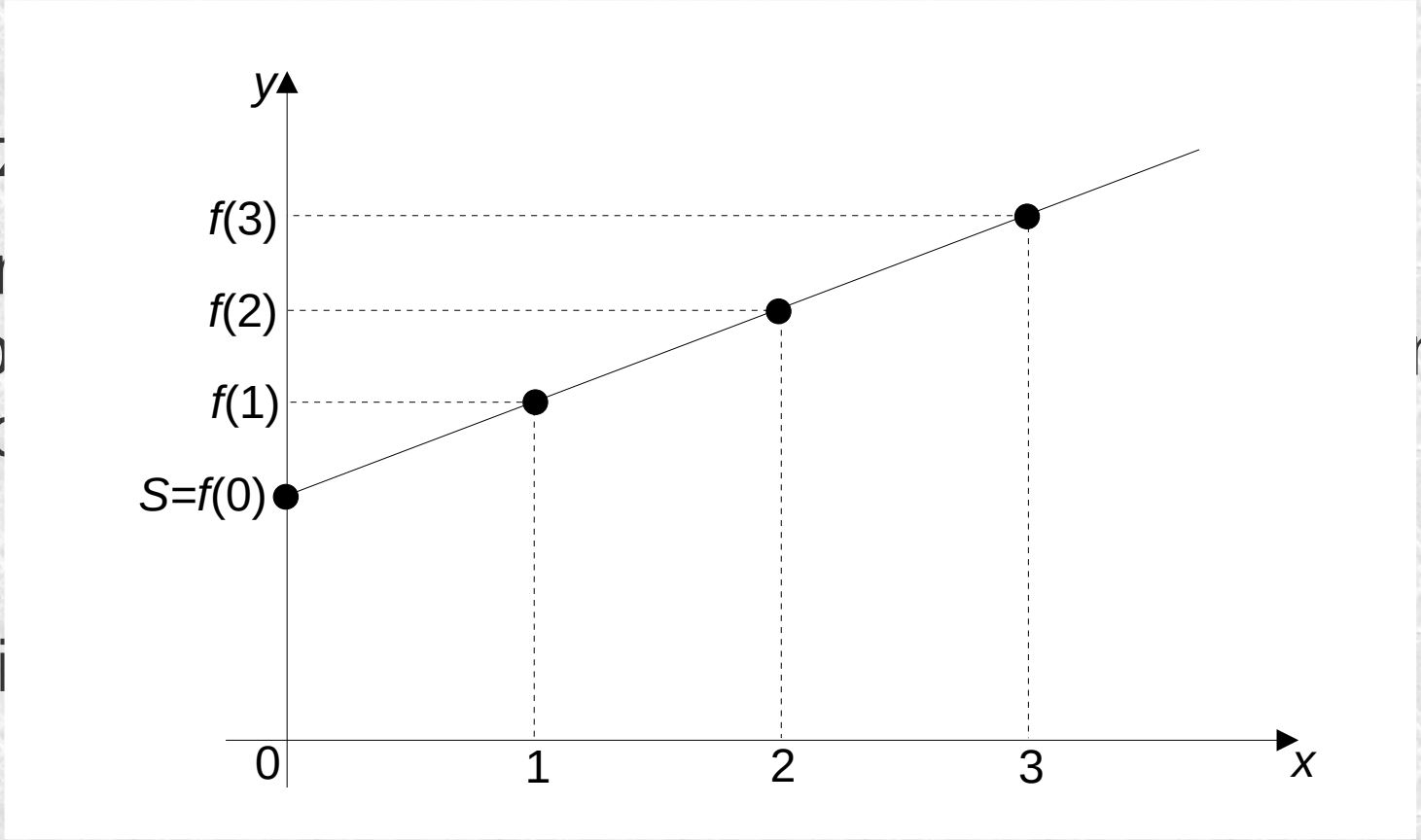
- razvil Adi Shamir leta 1979
- temelji na polinomski interpolaciji oz. lastnosti, da potrebujemo vsaj *K* točk za rekonstrukcijo polinoma stopnje *K*-1:

$$y=f(x)=a_{k-1}x^{k-1}+a_{k-2}x^{k-2}+...+a_0$$

- primer: (2,*N*)-pragovna shema
  - „polinom“ stopnje *K*-1=1 je premica
  - deleži in skrivnost so točke na premici; za rekonstrukcijo premice in izračun skrivnosti potrebujemo vsaj dva deleža*

Shamirjeva metoda

- raz
- ter da
  po noma
  sto
- pri
  - deleži in skrivnost so točke na premici; za rekonstrukcijo premice in izračun skrivnosti potrebujemo vsaj dva deleža*



Shamirjeva metoda

- osnovni postopek:
  1) izberemo praštevilo $P>S,N$
  2) tvorimo naključne celoštevilske vrednosti koeficientov $a_1,..,a_{k-1}<P$
  3) vrednost prostega koeficienta postavimo na vrednost skrivnosti: $a_0=S$
  4) za vsakega zaupnika i ($1\leq i\leq N$) izračunamo delež skrivnosti kot par $<i;f(i)>$, kjer je $f(i)$ vrednost polinoma $f(x)=a_{k-1}x^{k-1}+a_{k-2}x^{k-2}+...+a_0$
- primer: $S=145$, $K=3$, $N=4$
  - izberemo praštevilo npr. $P=947$
  - tvorimo koeficiente npr. $a_0=145$, $a_1=224$, $a_2=567$
  - izračunamo deleže <1;936>, <2;2861>, <3;5920> in <4;10113>

Shamirjeva metoda

- osnovni postopek:
  1) izberemo praštevilo $P>S,N$
  2) tvorimo naključne celoštevilske vrednosti koeficientov $a_1,..,a_{k-1}<P$
  3) vrednost prostega koeficienta postavimo na vrednost skrivnosti: $a_0=S$
  4) za vsakega zaupnika i ($1\leq i\leq N$) izračunamo delež skrivnosti kot par $<i;f(i)>$, kjer je $f(i)$ vrednost polinoma $f(x)=a_{k-1}x^{k-1}+a_{k-2}x^{k-2}+...+a_0$
- primer: $S=145$, $K=3$, $N=4$
  - izberemo praštevilo npr. $P=947$
  - tvorimo koeficiente npr. $a_0=145$, $a_1=224$, $a_2=567$
  - izračunamo deleže <1;936>, <2;2861>, <3;5920> in <4;10113>

$= 567\cdot 1^2 + 224\cdot 1^1 + 145$

Shamirjeva metoda

- osnovni postopek:
  1) izberemo praštevilo $P>S,N$
  2) tvorimo naključne celoštevilske vrednosti koeficientov $a_1,..,a_{k-1}<P$
  3) vrednost prostega koeficienta postavimo na vrednost skrivnosti: $a_0=S$
  4) za vsakega zaupnika i ($1\leq i\leq N$) izračunamo delež skrivnosti kot par $<i;f(i)>$, kjer je $f(i)$ vrednost polinoma $f(x)=a_{k-1}x^{k-1}+a_{k-2}x^{k-2}+...+a_0$
- primer: $S=145$, $K=3$, $N=4$
  - izberemo praštevilo npr. $P=947$
  - tvorimo koeficiente npr. $a_0=145$, $a_1=224$, $a_2=567$
  - izračunamo deleže <1;936>, <2;2861>, <3;5920> in <4;10113>

$= 567\cdot 2^2 + 224\cdot 2^1 + 145$

Shamirjeva metoda

- osnovni postopek:
  1) izberemo praštevilo $P>S,N$
  2) tvorimo naključne celoštevilske vrednosti koeficientov $a_1,..,a_{k-1}<P$
  3) vrednost prostega koeficienta postavimo na vrednost skrivnosti: $a_0=S$
  4) za vsakega zaupnika i ($1\leq i\leq N$) izračunamo delež skrivnosti kot par $<i;f(i)>$, kjer je $f(i)$ vrednost polinoma $f(x)=a_{k-1}x^{k-1}+a_{k-2}x^{k-2}+...+a_0$
- primer: $S=145$, $K=3$, $N=4$
  - izberemo praštevilo npr. $P=947$
  - tvorimo koeficiente npr. $a_0=145$, $a_1=224$, $a_2=567$
  - izračunamo deleže <1;936>, <2;2861>, <3;5920> in <4;10113>

$= 567\cdot 3^2 + 224\cdot 3^1 + 145$

Shamirjeva metoda

- osnovni postopek:
  1) izberemo praštevilo $P>S,N$
  2) tvorimo naključne celoštevilske vrednosti koeficientov $a_1,..,a_{k-1}<P$
  3) vrednost prostega koeficienta postavimo na vrednost skrivnosti: $a_0=S$
  4) za vsakega zaupnika i ($1\leq i\leq N$) izračunamo delež skrivnosti kot par $<i;f(i)>$, kjer je $f(i)$ vrednost polinoma $f(x)=a_{k-1}x^{k-1}+a_{k-2}x^{k-2}+...+a_0$
- primer: $S=145$, $K=3$, $N=4$
  - izberemo praštevilo npr. $P=947$
  - tvorimo koeficiente npr. $a_0=145$, $a_1=224$, $a_2=567$
  - izračunamo deleže <1;936>, <2;2861>, <3;5920> in <4;10113>

$= 567\cdot 4^2 + 224\cdot 4^1 + 145$

Shamirjeva metoda

- rekonstrukcija skrivnosti:
  1) s pomočjo znanih K deležev skrivnosti $\langle x_j; f(x_j)\rangle$ $(1 \le j \le K)$ lahko vrednost skrivnosti $S=a_0=f(0)$ izračunamo po enačbi:

$$S=\sum_{j=1}^{K} f(x_j) \prod_{\substack{m=1 \\ m\neq j}}^{K} \frac{x_m}{x_m - x_j}$$

- rekonstrukcija skrivnosti iz prejšnjega zgleda:
  - predpostavimo, da poznamo deleže <1;936>, <3;5920> in <4;10113>

$$S=f(x_1)\cdot\frac{x_2\cdot x_3}{(x_2-x_1)\cdot(x_3-x_1)}+f(x_2)\cdot\frac{x_1\cdot x_3}{(x_1-x_2)\cdot(x_3-x_2)}+f(x_3)\cdot\frac{x_1\cdot x_2}{(x_1-x_3)\cdot(x_2-x_3)}=$$

$$=936\cdot\frac{3\cdot 4}{(3-1)\cdot(4-1)}+5920\cdot\frac{1\cdot 4}{(1-3)\cdot(4-3)}+10113\cdot\frac{1\cdot 3}{(1-4)\cdot(3-4)}=$$

$$=936\cdot 2+5920\cdot(-2)+10113\cdot 1=145$$

Shamirjeva metoda

- rekonstrukcija skrivnosti:
  1) s pomočjo znanih K deležev skrivnosti $\langle x_j; f(x_j)\rangle$ $(1 \le j \le K)$ lahko vrednost skrivnosti $S=a_0=f(0)$ izračunamo po enačbi:

$$S=\sum_{j=1}^{K} f(x_j) \prod_{\substack{m=1 \\ m\neq j}}^{K} \frac{x_m}{x_m - x_j}$$

Lagrangeovi polinomi $L_j(0)$

- rekonstrukcija skrivnosti iz prejšnjega zgleda:
  - predpostavimo, da poznamo deleže <1;936>, <3;5920> in <4;10113>

$$S=f(x_1)\cdot\frac{x_2\cdot x_3}{(x_2-x_1)\cdot(x_3-x_1)}+f(x_2)\cdot\frac{x_1\cdot x_3}{(x_1-x_2)\cdot(x_3-x_2)}+f(x_3)\cdot\frac{x_1\cdot x_2}{(x_1-x_3)\cdot(x_2-x_3)}=$$

$$=936\cdot\frac{3\cdot 4}{(3-1)\cdot(4-1)}+5920\cdot\frac{1\cdot 4}{(1-3)\cdot(4-3)}+10113\cdot\frac{1\cdot 3}{(1-4)\cdot(3-4)}=$$

$$=936\cdot 2+5920\cdot(-2)+10113\cdot 1=145$$

Shamirjeva metoda

- slabost osnovnega postopka je, da zahteva 2 za (*K*,*N*)-pragovne sheme ni izpolnjena
  - s poznavanjem *K*-1 deležev lahko omejimo število možnih vrednosti skrivnosti
- rešitev: deleže izračunamo kot <*i*;*f*(*i*) mod *P*>, *P* se objavi
- isti primer: *S*=145, *K*=3, *N*=4, *P*=947, a_0=145, a_1=224, a_2=567
  - izračunani deleži so <1;936>, <2;20>, <3;238> in <4;643>

Shamirjeva metoda

- slabost osnovnega postopka je, da zahteva 2 za (*K*,*N*)-pragovne sheme ni izpolnjena
  - s poznavanjem *K*-1 deležev lahko omejimo število možnih vrednosti skrivnosti
- rešitev: deleže izračunamo kot <*i*;*f*(*i*) mod *P*>, *P* se objavi
- isti primer: *S*=145, *K*=3, *N*=4, *P*=947, a_0=145, a_1=224, a_2=567
  - izračunani deleži so <1;936>, <2;20>, <3;238> in <4;643>

= 2861 mod 947

Shamirjeva metoda

- slabost osnovnega postopka je, da zahteva 2 za (*K*,*N*)-pragovne sheme ni izpolnjena
  - s poznavanjem *K*-1 deležev lahko omejimo število možnih vrednosti skrivnosti
- rešitev: deleže izračunamo kot <*i*;*f*(*i*) mod *P*>, *P* se objavi
- isti primer: *S*=145, *K*=3, *N*=4, *P*=947, a_0=145, a_1=224, a_2=567
  - izračunani deleži so <1;936>, <2;20>, <3;238> in <4;643>
  - rekonstrukcija z deleži <1;936>, <3;238> in <4;643>:

$$S=\left(f(x_1)\cdot\frac{x_2\cdot x_3}{(x_2-x_1)\cdot(x_3-x_1)}+f(x_2)\cdot\frac{x_1\cdot x_3}{(x_1-x_2)\cdot(x_3-x_2)}+f(x_3)\cdot\frac{x_1\cdot x_2}{(x_1-x_3)\cdot(x_2-x_3)}\right)\bmod P=$$

$$=\left(936\cdot\frac{3\cdot 4}{(3-1)\cdot(4-1)}+238\cdot\frac{1\cdot 4}{(1-3)\cdot(4-3)}+643\cdot\frac{1\cdot 3}{(1-4)\cdot(3-4)}\right)\bmod 947=$$

$$=(936\cdot 2+238\cdot(-2)+643\cdot 1)\bmod 947=145$$

Shamirjeva metoda

- slabost osnovnega postopka je, da zahteva 2 za (*K*,*N*)-pragovne sheme ni izpolnjena
  - s poznavanjem *K*-1 deležev lahko omejimo število možnih vrednosti skrivnosti
- rešitev: deleže izračunamo kot <*i*;*f*(*i*) mod *P*>, *P* se objavi
- isti primer: *S*=145, *K*=3, *N*=4, *P*=947, a_0=145, a_1=224, a_2=567
  - izračunani deleži so <1;936>, <2;20>, <3;238> in <4;643>
  - rekonstrukcija z deleži <1;936>, <3;238> in <4;643>:

$$S=\left(f(x_1)\cdot\frac{x_2\cdot x_3}{(x_2-x_1)\cdot(x_3-x_1)}+f(x_2)\cdot\frac{x_1\cdot x_3}{(x_1-x_2)\cdot(x_3-x_2)}+f(x_3)\cdot\frac{x_1\cdot x_2}{(x_1-x_3)\cdot(x_2-x_3)}\right)\bmod P=$$

$$=\left(936\cdot\frac{3\cdot 4}{(3-1)\cdot(4-1)}+238\cdot\frac{1\cdot 4}{(1-3)\cdot(4-3)}+643\cdot\frac{1\cdot 3}{(1-4)\cdot(3-4)}\right)\bmod 947=$$

$$=145$$

OK, če se deljenja lepo izidejo

Shamirjeva metoda

- kadar se deljenje ne izide, upoštevamo naslednjo lastnost:

$$\frac{x}{y} \pmod{n} \equiv x \cdot y^{-1} \pmod{n}$$

Shamirjeva metoda

- kadar se deljenje ne izide, upoštevamo naslednjo lastnost:

$$\frac{x}{y} \pmod{n} \equiv x \cdot y^{-1} \pmod{n}$$

multiplikativni inverz od y (mod n)

Shamirjeva metoda

- kadar se deljenje ne izide, upoštevamo naslednjo lastnost:

$$\frac{x}{y} \pmod{n} \equiv x \cdot y^{-1} \pmod{n}$$

- zgled: K=3, N=4, S=137, P=241, a_0=137, a_1=225, a_2=180
  - izračunamo deleže <1;60>, <2;102>, <3;22> in <4;61>
  - rekonstrukcija iz deležev <1;60>, <2;102> in <4;61>

$$S = \left(f(x_1) \cdot \frac{x_2 \cdot x_3}{(x_2 - x_1) \cdot (x_3 - x_1)} + f(x_2) \cdot \frac{x_1 \cdot x_3}{(x_1 - x_2) \cdot (x_3 - x_2)} + f(x_3) \cdot \frac{x_1 \cdot x_2}{(x_1 - x_3) \cdot (x_2 - x_3)} \right) \bmod P =$$

$$= \left(60 \cdot \frac{2 \cdot 4}{(2-1) \cdot (4-1)} + 102 \cdot \frac{1 \cdot 4}{(1-2) \cdot (4-2)} + 61 \cdot \frac{1 \cdot 2}{(1-4) \cdot (2-4)} \right) \bmod 241 =$$

$$= (60 \cdot 8 \cdot 3^{-1} + 102 \cdot (-2) + 61 \cdot 1 \cdot 3^{-1}) \bmod 241 = (60 \cdot 8 \cdot 161 + 102 \cdot (-2) + 61 \cdot 1 \cdot 161) \bmod 241 = 137$$

Shamirjeva metoda

- med rekonstrukcijo skrivnosti lahko pride do numeričnih nestabilnosti v dveh primerih:
  - zaradi zaokrožitvene napake pri izračunu ulomkov
  - zaradi prekoračitev pri računanju produktov velikih števil
- rešitev:
  - pri izračunu ulomkov števec pred deljenjem množimo s produktom vrednosti v vseh imenovalcih, tako da so rezultati vedno celoštevilski; na koncu izvedemo delitev s to vrednostjo
  - vse člene vsote sproti računamo po modulu P, saj velja:

$$a \bmod P = c \Leftrightarrow a \equiv c \pmod{P},\ b \bmod P = d \Leftrightarrow b \equiv d \pmod{P}$$

$$(a+b) \equiv (c+d) \pmod{P} \Leftrightarrow$$
$$(a+b) \bmod P = (c+d) \bmod P = (a \bmod P + b \bmod P) \bmod P$$

Kitajski izrek o ostankih

- naj bodo $1<m_1<m_2<...<m_k$ paroma tuja cela števila za $k>1$
- naj bo $M=m_1 \cdot m_2 \cdot ... \cdot m_k$
- naj bodo s_i ($i=1..k$) poljubna pozitivna cela števila
- kitajski izrek o ostankih (Sun-Tzu, 3. st.):

  Pri zgornjih pogojih ima sistem enačb:

$$x \equiv s_1 \pmod{m_1}$$
$$x \equiv s_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv s_k \pmod{m_k}$$

  enolično rešitev $x \pmod M$, t.j. za vsak par rešitev x_1 in x_2 velja $x_1 \equiv x_2 \pmod M$

Kitajski izrek o ostankih

- postopek izračuna rešitve sistema modulskih enačb:
  1) izračunamo $z_i = M/m_i$ za i=1..k
  2) izračunamo multiplikativni inverz y_i od z_i (mod m_i) za i=1..k
  3) izračunamo $w_i = y_i \cdot z_i$ mod M za i=1..k
  4) enolična rešitev sistema je $x = (s_1w_1+s_2w_2+...+s_kw_k)$ mod M

Kitajski izrek o ostankih

- postopek izračuna rešitve sistema modulskih enačb:
  1) izračunamo $z_i = M/m_i$ za i=1..k
  2) izračunamo multiplikativni inverz y_i od z_i (mod m_i) za i=1..k
  3) izračunamo $w_i = y_i \cdot z_i$ mod M za i=1..k
  4) enolična rešitev sistema je $x = (s_1w_1+s_2w_2+...+s_kw_k)$ mod M
- zgled: poiščimo rešitev sistema:

$$x \equiv 9 \pmod{17}$$
$$x \equiv 14 \pmod{25}$$
$$x \equiv 10 \pmod{48}$$

Kitajski izrek o ostankih

- postopek izračuna rešitve sistema modulskih enačb:
  1) izračunamo $z_i = M/m_i$ za i=1..k
  2) izračunamo multiplikativni inverz y_i od z_i (mod m_i) za i=1..k
  3) izračunamo $w_i = y_i \cdot z_i$ mod M za i=1..k
  4) enolična rešitev sistema je $x = (s_1w_1+s_2w_2+...+s_kw_k)$ mod M
- zgled: poiščimo rešitev sistema:

$$x \equiv 9 \pmod{17} \qquad m_1 = 17^1$$
$$x \equiv 14 \pmod{25} \qquad m_2 = 5^2$$
$$x \equiv 10 \pmod{48} \qquad m_3 = 2^4 \cdot 3^1$$

Kitajski izrek o ostankih

- postopek izračuna rešitve sistema modulskih enačb:
  1) izračunamo $z_i = M/m_i$ za i=1..k
  2) izračunamo multiplikativni inverz y_i od z_i (mod m_i) za i=1..k
  3) izračunamo $w_i = y_i \cdot z_i$ mod M za i=1..k
  4) enolična rešitev sistema je $x = (s_1w_1+s_2w_2+...+s_kw_k)$ mod M
- zgled: poiščimo rešitev sistema:

$$x \equiv 9 \pmod{17}$$
$$x \equiv 14 \pmod{25}$$
$$x \equiv 10 \pmod{48}$$

$m_1=17^1$
$m_2=5^2$
$m_3=2^4 \cdot 3^1$

m_i so paroma tuja števila ✓

Kitajski izrek o ostankih

- postopek izračuna rešitve sistema modulskih enačb:
  1) izračunamo $z_i = M/m_i$ za i=1..k
  2) izračunamo multiplikativni inverz y_i od z_i (mod m_i) za i=1..k
  3) izračunamo $w_i = y_i \cdot z_i$ mod M za i=1..k
  4) enolična rešitev sistema je $x = (s_1w_1+s_2w_2+...+s_kw_k)$ mod M
- zgled: poiščimo rešitev sistema:

$$x \equiv 9 \pmod{17}$$
$$x \equiv 14 \pmod{25}$$
$$x \equiv 10 \pmod{48}$$

$m_1=17^1$, $m_2=5^2$, $m_3=2^4 \cdot 3^1$

m_i so paroma tuja števila ✓

m_1=17, m_2=25, m_3=48, M=20400, s_1=9, s_2=14, s_3=10

Kitajski izrek o ostankih

- postopek izračuna rešitve sistema modulskih enačb:
  1) izračunamo $z_i = M/m_i$ za i=1..k
  2) izračunamo multiplikativni inverz y_i od z_i (mod m_i) za i=1..k
  3) izračunamo $w_i = y_i \cdot z_i$ mod M za i=1..k
  4) enolična rešitev sistema je $x = (s_1w_1+s_2w_2+...+s_kw_k)$ mod M
- zgled: poiščimo rešitev sistema:

  m_1=17, m_2=25, m_3=48, M=20400, s_1=9, s_2=14, s_3=10

  1) z_1=1200, z_2=816, z_3=425

Kitajski izrek o ostankih

- postopek izračuna rešitve sistema modulskih enačb:
  1) izračunamo $z_i = M/m_i$ za i=1..k
  2) izračunamo multiplikativni inverz y_i od z_i (mod m_i) za i=1..k
  3) izračunamo $w_i = y_i \cdot z_i$ mod M za i=1..k
  4) enolična rešitev sistema je $x = (s_1w_1+s_2w_2+...+s_kw_k)$ mod M
- zgled: poiščimo rešitev sistema:

$$m_1=17,\ m_2=25,\ m_3=48,\ M=20400,\ s_1=9,\ s_2=14,\ s_3=10$$

1) $z_1=1200,\ z_2=816,\ z_3=425$
2) rešujemo enačbe oblike $y_i \equiv z_i^{-1}$ (mod m_i):

$y_1 \equiv 1200^{-1} \pmod{17} \equiv 10^{-1} \pmod{17} \equiv -5 \pmod{17} \equiv 12 \pmod{17}$*
$y_2 \equiv 816^{-1} \pmod{25} \equiv 16^{-1} \pmod{25} \equiv 11 \pmod{25}$
$y_3 \equiv 425^{-1} \pmod{48} \equiv 41^{-1} \pmod{48} \equiv 41 \pmod{48}$

Kitajski izrek o ostankih

korak	kvocient	ostanek	substitucija	kombiniran izraz
1		10		10=10·1+17·0
2		17		17=10·0+17·1
3	0	10=10-17·0	10=(10·1+17·0)-(10·0+17·1)·0	10=10·1+17·0
4	1	7=17-10·1	7=(10·0+17·1)-(10·1+17·0)·1	7=10·(-1)+17·1
5	1	3=10-7·1	3=(10·1+17·0)-(10·(-1)+17·1)·1	3=10·2+17·(-1)
6	2	1=7-3·2	1=(10·(-1)+17·1)-(10·2+17·(-1))·2	1=10·(-5)+17·3
7	3	0		

1) $z_1=1200$, $z_2=816$, $z_3=425$

2) rešujemo enačbe oblike $y_i \equiv z_i^{-1} \pmod{m_i}$:

$y_1 \equiv 1200^{-1} \pmod{17} \equiv 10^{-1} \pmod{17} \equiv -5 \pmod{17} \equiv 12 \pmod{17}$*

$y_2 \equiv 816^{-1} \pmod{25} \equiv 16^{-1} \pmod{25} \equiv 11 \pmod{25}$

$y_3 \equiv 425^{-1} \pmod{48} \equiv 41^{-1} \pmod{48} \equiv 41 \pmod{48}$

Kitajski izrek o ostankih

- postopek izračuna rešitve sistema modulskih enačb:
  1) izračunamo $z_i = M/m_i$ za i=1..k
  2) izračunamo multiplikativni inverz y_i od z_i (mod m_i) za i=1..k
  3) izračunamo $w_i = y_i \cdot z_i$ mod M za i=1..k
  4) enolična rešitev sistema je $x = (s_1w_1+s_2w_2+...+s_kw_k)$ mod M
- zgled: poiščimo rešitev sistema:

  m_1=17, m_2=25, m_3=48, M=20400, s_1=9, s_2=14, s_3=10

  1) z_1=1200, z_2=816, z_3=425
  2) y_1=12, y_2=11, y_3=41
  3) w_1=14400, w_2=8976, w_3=17425

Kitajski izrek o ostankih

- postopek izračuna rešitve sistema modulskih enačb:
  1) izračunamo $z_i = M/m_i$ za i=1..k
  2) izračunamo multiplikativni inverz y_i od z_i (mod m_i) za i=1..k
  3) izračunamo $w_i = y_i \cdot z_i$ mod M za i=1..k
  4) enolična rešitev sistema je $x = (s_1w_1+s_2w_2+...+s_kw_k)$ mod M
- zgled: poiščimo rešitev sistema:

  m_1=17, m_2=25, m_3=48, M=20400, s_1=9, s_2=14, s_3=10

  1) z_1=1200, z_2=816, z_3=425
  2) y_1=12, y_2=11, y_3=41
  3) w_1=14400, w_2=8976, w_3=17425
  4) x = 429514 mod 20400 = 1114

Kitajski izrek o ostankih

- kitajski izrek lahko uporabimo za implementacijo (K,N)-pragovne sheme za delitev skrivnosti S:
  - izbrati je potrebno naraščajoče zaporedje N paroma tujih si števil m_i, tako da je S manjša od produkta katerihkoli K izmed njih in večja od produkta katerihkoli K-1 izmed njih
    - obstajata dve shemi izbire m_i – Mignotte in Asmuth-Bloom
  - deleži skrivnosti so pari $<s_i;m_i>$, kjer se s_i izračuna po shemi
  - skrivnost lahko rekonstruiramo s poznavanjem vsaj K deležev (z indeksi i_1, i_2, ..., i_K) tako, da rešimo sistem enačb:

$$x \equiv s_{i1} \pmod{m_{i1}}$$
$$x \equiv s_{i2} \pmod{m_{i2}}$$
$$\vdots$$
$$x \equiv s_{iK} \pmod{m_{iK}}$$

  in postavimo $S = x \bmod M$

Mignottejeva shema

- zaporedje $1<m_1<m_2<\ldots<m_N$ so paroma tuja si števila (običajno praštevila), izbrana tako, da:
  1) je produkt najmanjših K števil večji od produkta največjih K-1:

$$\alpha = \prod_{i=N-K+2}^{N} m_i \qquad \beta = \prod_{i=1}^{K} m_i \qquad \alpha < \beta$$

  2) je skrivnost S vrednost z intervala (α,β)
- deleži se izračunajo kot $\mathbf{s_i = S \bmod m_i}$
- primer: [5,7,11,13,17] je Mignottejevo zaporedje za:
  - (2,5)-pragovno shemo, ker $17<5\cdot7=35$; skrivnost je lahko število z intervala (17,35)
  - (3,5)-pragovno shemo, ker $13\cdot17=221<5\cdot7\cdot11=385$; skrivnost je lahko število z intervala (221,385)
  - (4,5)-pragovno shemo, ker $11\cdot13\cdot17=2431<5\cdot7\cdot11\cdot13=5005$; skrivnost je lahko število z intervala (2431,5005)

Mignottejeva shema

- zaporedje $1<m_1<m_2<...<m_N$ so paroma tuja si števila (običajno praštevila), izbrana tako, da:
  1) je produkt najmanjših K števil večji od produkta največjih K-1:

$$\alpha = \prod_{i=N-K+2}^{N} m_i \qquad \beta = \prod_{i=1}^{K} m_i \qquad \alpha < \beta$$

  2) je skrivnost S vrednost z intervala (α,β)
- deleži se izračunajo kot $\boldsymbol{s_i = S \bmod m_i}$
- primer: skrivnost S=1234567 želimo deliti s (5,7)-pragovno shemo
  - potrebujemo Mignottejevo zaporedje dolžine N=7, tako da bo produkt β najmanjših K=5 števil večji od produkta α največjih K-1=4, pri čemer mora veljati $\alpha < S < \beta$
  - tem pogojem ustreza npr. zaporedje [7,17,19,23,31,37,41], ker α=23·31·37·41=1081621 < 1234567 < β=7·17·19·23·31=1612093

Mignottejeva shema – zgled

- $[m_i]=[5,7,11,13,17]$, $K=3$, $N=5$, $S=299$
- tvorba deležev: $s_1=299 \bmod 5=4$, $s_2=5$, $s_3=2$, $s_4=0$, $s_5=10$
- rekonstrukcija iz deležev $\langle s_1;m_1\rangle$, $\langle s_3;m_3\rangle$ in $\langle s_5;m_5\rangle$:

$$x\equiv 4 \pmod 5$$
$$x\equiv 2 \pmod{11}$$
$$x\equiv 10 \pmod{17}$$

$m_1=5$, $m_3=11$, $m_5=17$, $M=935$, $s_1=4$, $s_3=2$, $s_5=10$

1) $z_1=187$, $z_3=85$, $z_5=55$
2) $y_1=3$, $y_3=7$, $y_5=13$
3) $w_1=561$, $w_3=595$, $w_5=715$
4) $S = (4\cdot 561+2\cdot 595+10\cdot 715) \bmod 935 = 10584 \bmod 935 = 299$

Asmuth-Bloomova shema

- problem Mignottejeve sheme: z manj kot K deleži lahko omejimo nabor možnih S; to težavo odpravlja Asmuth-Bloomova shema
- zaporedje $m_0<m_1<m_2<...<m_N$ so paroma tuja si števila (običajno praštevila), izbrana tako, da velja:

$$\alpha = m_0 \cdot \prod_{i=N-K+2}^{N} m_i \qquad \beta = \prod_{i=1}^{K} m_i \qquad \alpha < \beta$$

- skrivnost S je vrednost z intervala $[0,m_0-1]$; m_0 je lahko javen
- deleži se izračunajo kot $\boldsymbol{s_i = (S+\eta \cdot m_0) \bmod m_i}$, kjer je η naključno naravno število, tako da $S+\eta \cdot m_0<m_1 \cdot m_2 \cdot ... \cdot m_K$
- primer: [11,17,29,31,41] je A.-B. zaporedje za:
  - (2,4)-pragovno shemo, ker $11 \cdot 41=451<17 \cdot 29=493$
  - (3,4)-pragovno shemo, ker $11 \cdot 31 \cdot 41=13981<17 \cdot 29 \cdot 31=15283$

Asmuth-Bloomova shema

- problem Mignottejeve sheme: z manj kot K deleži lahko omejimo nabor možnih S; to težavo odpravlja Asmuth-Bloomova shema
- zaporedje $m_0<m_1<m_2<...<m_N$ so paroma tuja si števila (običajno praštevila), izbrana tako, da velja:

$$\alpha = m_0 \cdot \prod_{i=N-K+2}^{N} m_i \qquad \beta = \prod_{i=1}^{K} m_i \qquad \alpha < \beta$$

- skrivnost S je vrednost z intervala $[0,m_0-1]$; m_0 je lahko javen
- deleži se izračunajo kot $\boldsymbol{s_i = (S+\eta \cdot m_0) \bmod m_i}$, kjer je η naključno naravno število, tako da $S+\eta \cdot m_0<m_1 \cdot m_2 \cdot ... \cdot m_K$
- primer: skrivnost S=12345 želimo deliti s (3,5)-pragovno shemo
  - izberemo $m_0>S$, npr. prvo večje praštevilo m_0=12347
  - pogojem Asmuth-Bloomovega zaporedja za (3,5)-pragovno shemo ustreza npr. [12347,20011,20021,20023,20029,20047], ker $12347 \cdot 20029 \cdot 20047<20011 \cdot 20021 \cdot 20023$

Asmuth-Bloomova shema - zgled

- $[m_i]=[11,17,29,31,41]$, $K=2$, $N=4$, $S=9$
- $m_1 \cdot m_2=493$, zato izberemo naključen η, tako da $9+\eta \cdot 11<493$, npr. $\eta=32$
- tvorba deležev: $s_1=361 \bmod 17=4$, $s_2=13$, $s_3=20$, $s_4=33$
- rekonstrukcija iz deležev $<s_1;m_1>$ in $<s_3;m_3>$:

$$x \equiv 4 \pmod{17}$$
$$x \equiv 20 \pmod{31}$$

$m_1=17$, $m_3=31$, $M=527$, $s_1=4$, $s_3=20$

1) $z_1=31$, $z_3=17$
2) $y_1=11$, $y_3=11$
3) $w_1=341$, $w_3=187$
4) $S+\eta \cdot m_0 = (4 \cdot 341+20 \cdot 187) \bmod 527 = 5104 \bmod 527 = 361$
5) $S = 361 \bmod m_0 = 361 \bmod 11 = 9$