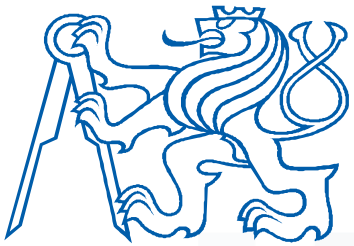
České vysoké učení technické v Praze
Fakulta elektrotechnická
Katedra telekomunikační techniky

A7B32KBE – 7.přednáška

Kryptosystémy veřejného klíče II

Ing. Tomáš Vaněk, Ph.D. tomas.vanek@fel.cvut.cz



Obsah

- EC nad R
- EC nad polem F_p
- EC polem F_2^m
- ECC – Elliptic Curve Cryptosystems
  - ECDH
  - PSEC
- HEC – Hyperelliptic Curve Cryptosytem
- Algoritmy „Suite B“

EC - úvod

- Eliptická křivka (EC) je množina bodů, která vyhovuje rovnici eliptické funkce.
- Eliptické křivky jsou speciální podtřídou kubických křivek.
- Zkoumáním vlastností eliptických křivek se nejvíce zabýval přední německý matematik 19. století Karl Theodor Wilhelm Weierstrass
- Název eliptické vznikl proto, že kubické rovinné funkce se v minulosti používaly k výpočtu obvodu elipsy (eliptický integrál).
- V roce 1985 přišli Victor Miller a Neal Koblitz na možnost použití eliptických křivek v rámci kryptosystému veřejného klíče (ECC).

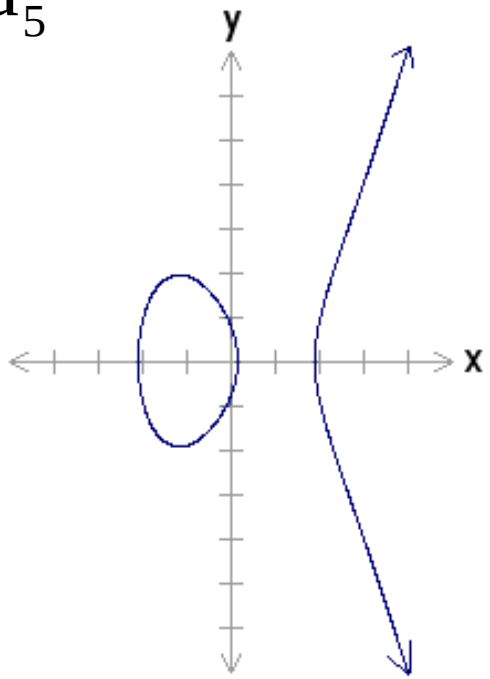
EC nad reálnými čísly

Eliptickou křivka nad množinou reálných čísel je obecně definována jako množina bodů (x,y) vyhovujících rovnici ve tvaru: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_5$

Kde $x, y, a_1, a_2, a_3, a_4, a_5 \in \mathbb{R}$

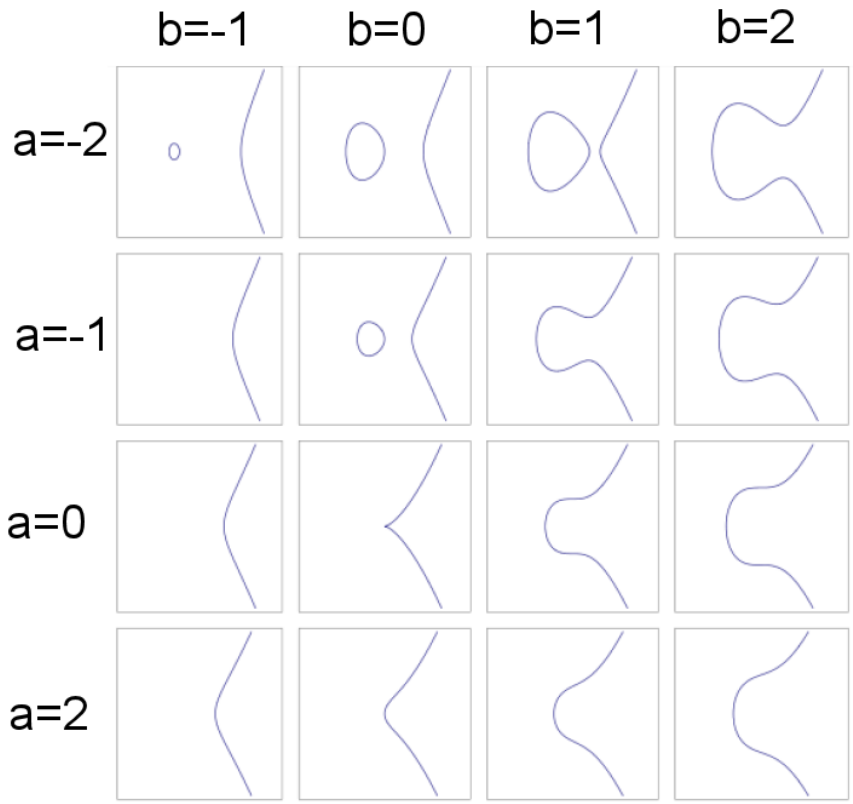
Každou křivku lze převést na tvar:

$$y^2 = x^3 + ax + b$$

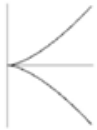


Eliptická křivka je jednoznačně určena volbou koeficientů *a*,*b*.
Na příklad pro *a= -4* a *b=0,67*
dostaneme eliptickou křivku popsanou rovnicí $y^2 = x^3 - 4x + 0{,}67$

Graf EC na množinou R



uzlová singularita



hrotová singularita

EC nad reálnými čísly

- Eliptická křivka může tvořit grupu, pokud není singulární,

  tzn. člen x^3+ax+b je nerozložitelný, neboli pokud platí, že $4a^3+27b^2\neq 0$
- Grupa na EC nad reálnými čísly se skládá z bodů odpovídajících bodům na eliptické křivce a z jednoho speciálního bodu – O nazvaného „bod v nekonečnu“.
- Bod O plní funkci nulového prvku.
- Grupy na eliptických křivkách jsou aditivní - základní definovanou operací je „sčítání“.
- Početní operace jsou definovány geometricky.
- Tato operace nemá s normálním sčítáním tak, jak ho známe mnoho společného !

EC nad reálnými čísly

- Inverzním bodem k bodu $P = (x_P, y_P)$ je jeho zrcadlový obraz podle osy x, $-P = (x_P, -y_P)$.
- Každý bod $-P$, inverzní k bodu P ležícím na eliptické křivce, leží také na téže eliptické křivce.
- Operace s eliptickými křivkami můžeme popsat dvěma způsoby:
  - geometricky
    - vhodný k výkladu pro svou názornost, ale nehodí se k výpočtům
  - algebraicky
    - není příliš názorný, ale je vhodný k výpočtům

EC – sčítání bodů P,Q – geometrický přístup

Nechť $P=(x_p,y_p)$, $Q=(q_x,q_y)$, $P \neq Q$ leží na společné EC.

Součet bodů P, Q probíhá ve dvou krocích.

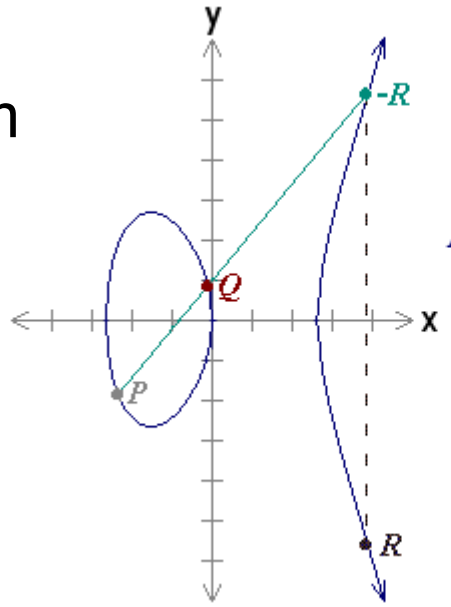
1) sestrojíme přímku procházející body P, Q, která protne eliptickou křivku právě v jednom bodě,

který nazveme -R.

2) bod -R je zrcadlovým obrazem bodu R podle osy x

Operace sčítání v grupě na eliptické křivce se zapisuje:

P + Q = R.



P (-2,35; -1,86)
Q (-0,1; 0,836)
- R (3,89; 5.62)
R (3,89; -5.62)
P + Q = R = (3,89; -5,62)

EC – sčítání bodů P,Q – albegraický přístup

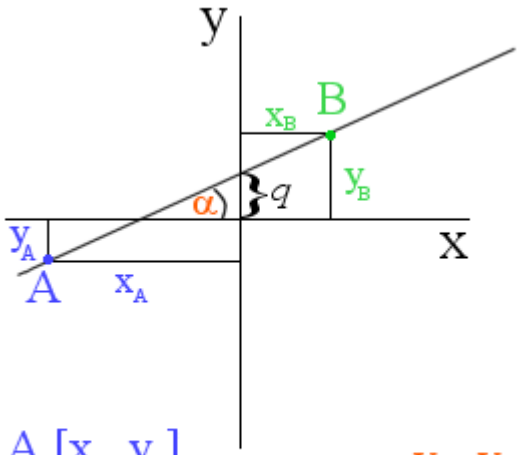
Nechť $P = (x_P, y_P)$ a $Q = (x_q, y_q)$ takové že, $P \neq Q$, pak součet $P + Q = R$, kde $R = (r_x, r_y)$

$$x_r = s^2 - x_p - x_q \qquad y_r = s(x_p - x_r) - y_p$$

$$s = \frac{y_p - y_q}{x_p - x_q}$$

EC – odvození rovnic pro sčítání bodů P a Q

- vyjdeme z geometrického vyjádření
- přímka procházející body P,Q je popsána analytickou rovnicí ve tvaru $Y = sX + q$, kde s je směrnice přímky a q je y-ová hodnota souřadnice v bodě protínajícím osu y (x=0)
- směrnice s vyjadřuje sklon přímky vůči souřadné soustavě



$$s = tg\alpha = \frac{y_A - y_B}{x_A - x_B}$$

A $[x_A, y_A]$

B $[x_B, y_B]$

$$tg\,\alpha = \frac{y_A - y_B}{x_A - x_B}$$

EC – odvození rovnic pro sčítání bodů P a Q

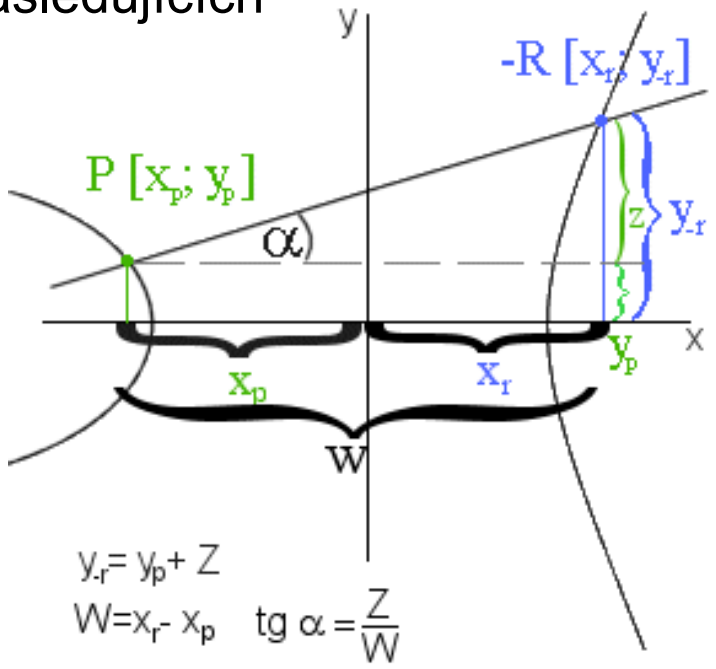
- Přímka protíná křivku právě ve třech bodech. Jsou to body P,Q a –R.
- Protože R a –R jsou zrcadlové podle osy x, tak jejich x-ové souřadnice se rovnají ($x_R = x_{-R}$). Proto má bod –R v následujících výpočtech souřadnice $-R=(x_R;y_{-R})$.

Jak je patrné na obrázku , tak

$$y_{-R} = y_P + Z$$

$$tg\ \alpha = \frac{Z}{W} = s$$

$$W = x_r - x_p$$



Po dosazení a vyjádření Z dostaneme rovnici $y_{-R} = y_P + s \cdot (x_R - x_P)$ To je rovnice pro y-ovou složku bodu –R. vynásobit –1 a dostaneme hledaný vztah pro y-ou složku bodu R $y_R = -y_P - s \cdot (x_R - x_P)$

EC – Sčítání bodů P a –P

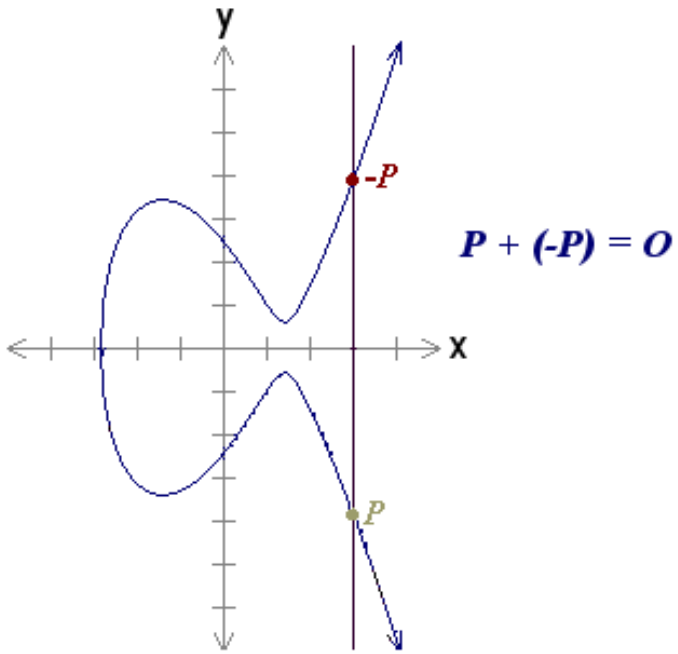
Přímka vedená skrz body P a -P je kolmá na osu *x* a neprotíná eliptickou křivku v žádném dalším bodu, a sčítání bodů P, -P není možné provést stejně jako v předchozím případě. Pro tento případ obsahuje grupa na eliptické křivce bod O - „bod v nekonečnu“.

$$P + (-P) = O.$$

V grupě eliptické křivky platí, že $P + O = P$.

O je identickým prvkem pro sčítání v grupě na EC.

Všechny EC mají identický prvek O pro operaci sčítání.



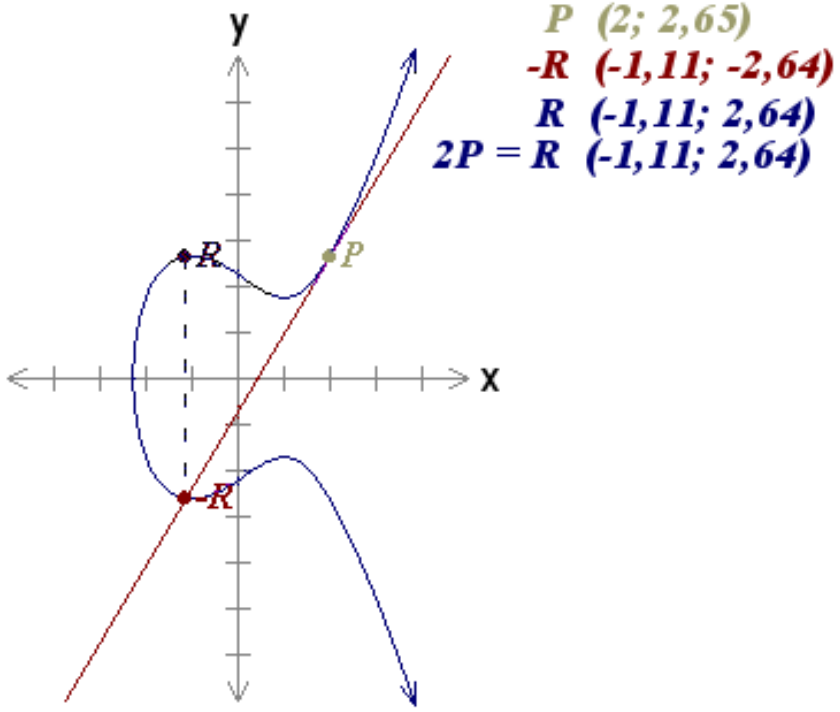
EC – zdvojení bodu P - geometrický přístup

Při součtu bodu P k sobě samému, se tečna ke křivce dotýká bodu P.

Pokud $y_P \neq 0$, pak tečna protíná EC právě v jednom bodu, -R.

-R je zrcadlový obraz R podle osy *x*. Tato operace se nazývá zdvojení bodu P.

P + P = 2P = R.



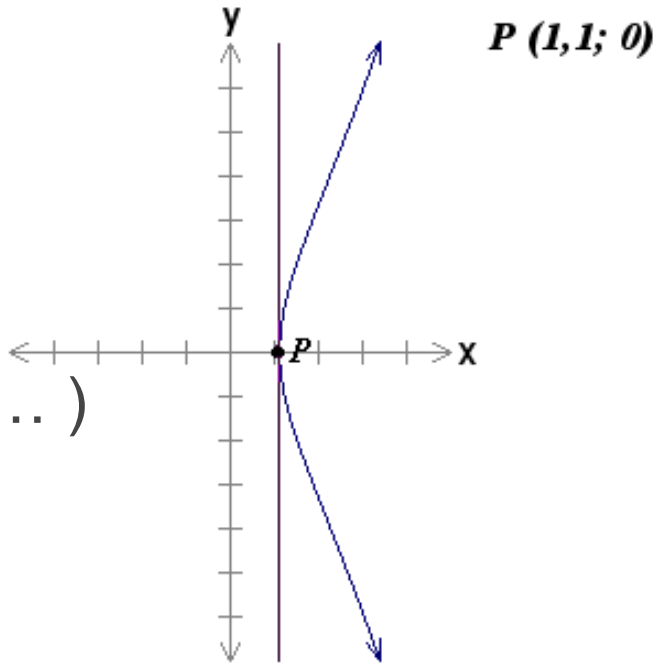
EC – zdvojení bodu P pokud $y_p=0$

Pokud bod $P = (x_P, y_P)$ je takový, že $y_P \neq 0$, pak tečna k P je kolmá na osu x a neprotíná eliptickou křivku v žádném dalším bodu.
Podle definice $2P = O$ pro každý takový bod P.

Bod 3P dostaneme součtem bodu 2P a P. Výsledkem je bod P, protože:

$$P + O = P.$$

Tedy 3P = P.
(a tak dále 4P=O, 5P=P, 6P=O, 7P=P, …)



EC nad konečnými poli

- Výpočty nad množinou reálných čísel jsou pomalé a díky zaokrouhlovacím chybám i nepřesné.
- Kryptografické aplikace vyžadují rychlé a přesné výpočty, proto se v praxi používají grupy na eliptických křivkách nad konečnými poli typu F_P a F_2^m.
- Konečný počet prvků grupy je nutnou vlastností grup používaných v kryptografii.

- Eliptickou křivku nad podložním polem F_P je možné definovat jako množinu bodů *(x,y)* vyhovujících rovnici

$$y^2 \bmod p = x^3 + ax + b \bmod p$$ (p je prvočíslo)

- Prvky pole F_p jsou čísla zbytkové třídy mod p. Počítá se s nimi stejně jako s EC nad $\boldsymbol{R}$, pouze přibude mod p.

EC nad konečnými poli

- Aby bylo možné na eliptické křivce nad F_P vytvořit grupu, je nutné aby člen $x^3 + ax + b$ byl nerozložitelný nebo, což je ekvivalentní, aby $4a^3 + 27b^2 \neq 0$
- Grupa na EC nad F_P, obsahuje
  - body odpovídající eliptické
  - speciální bod O - „bod v nekonečnu“
- EC nad F_P je tvořena konečným počtem bodů

- #E(F_P) řád křivky – celkový počet bodů tvořících EC + O
- n - řád bodu – nejmenší číslo n, pro které platí $n \cdot P = O$
- generátor - prvek EC, jehož mocninami lze vyjádřit libovolný prvek EC
- kofaktor – podíl řádu EC a prvočíselného dělitele

EC nad konečným polem typu Fp - PŘÍKLAD

- uvažujme EC nad polem F_{23}
- pro parametry $a = 1$ a $b = 0$, se obecná rovnice EC zjednoduší na tvar $y^2 \bmod 23 = x^3 + x \bmod 23$
- této rovnici vyhovuje následujících 23 bodů:
  (0,0) (1,5) (1,18) (9,5) (9,18) (11,10),(11,13) (13,5) (13,18) (15,3) (15,20) (16,8) (16,15) (17,10) (17,13) (18,10),(18,13) (19,1) (19,22) (20,4) (20,19) (21,6) (21,17)

a tedy řád křivky popsané rovnicí $y^2 = x^3 + x$ nad F_{23} je 23

- značíme $\#E(F_{23}) = 23$

- ! V tomto příkladu je náhodou řád křivky roven prvočíslu definujícímu velikost pole, při volbě jiných parametrů a,b by tomu tak již nebylo!

EC nad konečným polem typu Fp - PŘÍKLAD

Graf EC popsané rovnicí $y^2 = x^3 + x$

Graf není spojitý, protože křivku nad F_P tvoří jen konečný počet bodů.

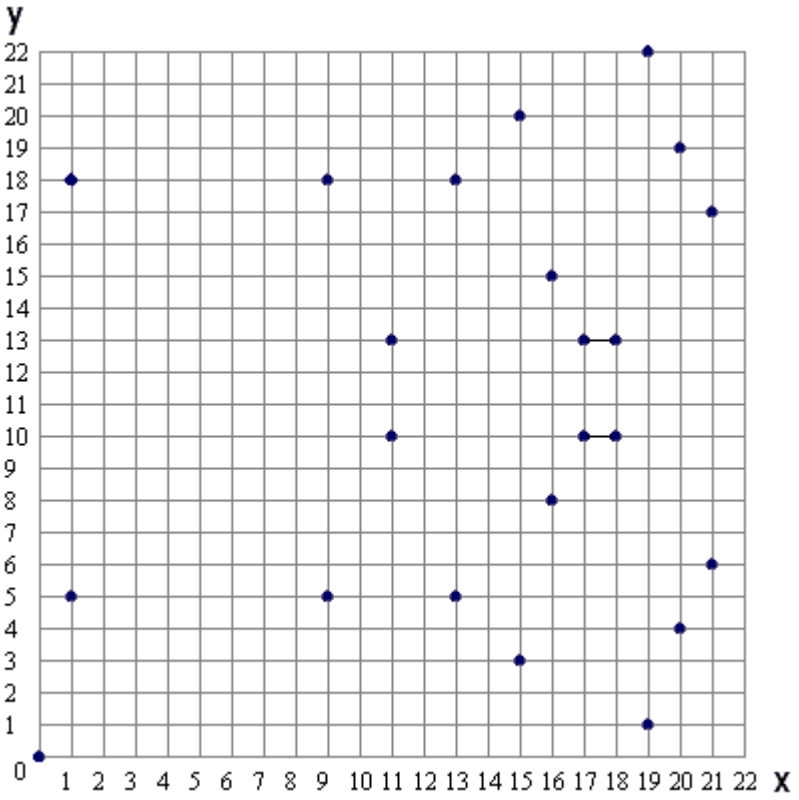
Například bod (9,5) vyhovuje této rovnici protože:

$y^2 \bmod p = x^3 + x \bmod p$

$5^2 \bmod 23 = 9^3 + 9 \bmod 23$

$25 \bmod 23 = 738 \bmod 23$

$2 = 2$



EC nad konečným polem typu Fp - aritmetika

Nechť $P = (x_P, y_P)$ a $Q = (x_q, y_q)$ takové že, $P \neq Q$,

$P + Q = R$, kde $x_r = s^2 - x_p - x_q \bmod p$

$$y_r = -y_p + s(x_p - x_r) \bmod p$$

$$s = \frac{y_p - y_q}{x_p - x_q} \bmod p$$

Pozn. s je směrnice přímky protínající body P a Q

EC nad konečným polem typu Fp – zdvojení bodu P

Nechť $P = (x_P, y_P)$; $2P = R$, kde

$$x_r = s^2 - 2x_p \bmod p$$

$$y_r = -y_p + s(x_p - x_r) \bmod p$$

$$s = \frac{3x_p^2 + a}{2y_p} \bmod p$$

Pozn.: a je jeden z parametrů, které určují eliptickou křivku a s je směrnice přímky protínající P a Q.

EC nad konečným polem typu Fp – násobení bodu

- realizováno dvěma základními operacemi
  - zdvojení bodu
  - sčítání bodů
- skalární násobení bodu P

$$Q = k \cdot P = \overbrace{P + P + P ... + P}^{k-krát}$$

$$P, Q \in E \quad k \in Z^{+}$$

- lze urychlit pomocí zdvojování – DAA („double and add“)

Příklad: Dány souřadnice bodu P, k =23. Určete Q

$$Q = k \cdot P = 23 \cdot P = 2 \cdot (2 \cdot (2 \cdot (2 \cdot P) + P) + P) + P$$

EC nad konečným polem typu Fp

Příklad: Mějme křivku E nad polem Fp a bod P ležící na ní.
Provádějme opakované sčítání bodu P k bodu P.

2P=P+P

3P=2P+P

…

- Libovolný bod Q vzniklý z takovéhoto výpočtu lze vyjádřit jako $Q=nP$, kde n udává počet sčítání.
- Protože EC má konečný počet bodů, musí se po určitém počtu kroků tato posloupnost zacyklit.
- Existuje takové n, pro které $nP=O$
- Nejmenší n, pro které platí $nP = O$, se nazývá řád bodu P.
- V praxi vybíráme takový bod, jehož řád je roven největšímu prvočíslu v rozkladu čísla #E (pro *n řádově* 2^{256}, dostaneme velmi dlouhou posloupnost, než se „zacyklí“) nebo jeho násobku (tzv. kofaktor)

EC nad konečným polem typu Fp – PŘÍKLAD

- uvažujme EC $y^2 = x^3 + x$ nad polem F_{23} a bod P=(9,5)

Spočítejte souřadnice bodu $Z(x_z,y_z) = 5P$

1) 5P=2*2P+P

2) výpočet 2P

$$s = \frac{3x_p^2 + a}{2y_p} \bmod p$$

$$x_r = s^2 - 2x_p \bmod p$$

$$y_r = -y_p + s(x_p - x_r) \bmod p$$

s=(3*9^2 +1)/2*5 mod 23 ≡ 244*7 mod 23 ≡ 6 mod 23

x_r=6^2-2*9 mod 23 ≡ 18 mod 23

y_r=-5+6(9-18) mod 23 ≡ 10 mod 23

- 2P=(18,10)

3) Výpočet 4P

s=(3*18^2 +1)/2*10 mod 23 ≡ 973*15 mod 23 ≡ 13 mod 23

x_r=13^2-2*18 mod 23 ≡ 18 mod 23

y_r=-10+13(18-18) mod 23 ≡ 13 mod 23

- 4P=(18,13)

4) Výpočet 5P

$$s = \frac{y_p - y_q}{x_p - x_q} \bmod p$$

$$x_r = s^2 - x_p - x_q \bmod p$$

$$y_r = -y_p + s(x_p - x_r) \bmod p$$

s=(5-13)/(9-18)mod 23 ≡ -8/-9 mod 23 ≡ 15/14mod23 ≡ 6 mod 23

x_r=6^2-9-18 mod 23 ≡ 9 mod 23

y_r=-5+6(9-9) mod 23 ≡ 18 mod 23

- 5P=(9,18)

EC nad konečným polem typu F_2^m

- Prvky pole F_2^m jsou polynomy o stupni menším než m.
- Prvky pole typu F_2^m jsou binární řetězce (vektory) délky m.
- Číslo **m** se nazývá **řád** pole.
- Koeficienty polynomů jsou v F_2 , to znamená, že nabývají hodnot 0 nebo 1. Prvky pole je také možno popsat vektorovém ve tvaru.
- Protože při výpočtech v F_2^m pracujeme s binárními řetězci, je pole tohoto typu velmi vhodné k počítačovému zpracování.
- Eliptická křivka vytvořená nad polem typu F_2^m je určena výběrem dvou parametrů a, b z množiny F_2^m ($b \neq 0$)

EC nad konečným polem typu F_2^m

Kvůli tomu, že prvky pole mají binární formu, rovnice EC má tvar:

$$y^2 + xy = x^3 + ax^2 + b$$

Eliptickou křivku tvoří body (x,y) vyhovující rovnici eliptické křivky nad F_2^m, kde x a y jsou prvky F_2^m.

Grupa na eliptické křivce nad podložním polem F_2^m obsahuje body odpovídající eliptické křivce a speciální bod O – „bod v nekonečnu“.

Eliptická křivka nad F_2^m je tvořena konečným počtem bodů.

Sčítání na EC nad konečným polem typu F_2^m

Příklad: Mějme dva polynomy $A = x^3+x^2+1$ and $B = x^2+x$.
Součet polynomů $A+B = x^3+2x^2+x+1$. Protože koeficienty jsou v mod 2, výsledek je $A+B= x^3+x+1$.

- Tentýž příklad s použitím vektorů pro zápis polynomů:
  $A = 1101_2$ $B = 0110_2$ $A + B = 1011_2$

- Protože koeficienty prvků pole jsou v F_2, sčítání prvků a, b v poli F_2^m ($a+b=c \bmod 2$) lze zjednodušit na $a \oplus b = c$

Závěr: Sčítání v poli F_2^m se realizuje operací XOR.

Odčítání na EC nad konečným polem typu F_2^m

- Protože sčítání se realizuje operací XOR platí, že :
  všechny prvky pole F_2^m jsou svojí vlastní aditivní inverzí protože:
  $(a_{m-1}a_{m-2}a_{m-3}\ldots a_1a_0) + (a_{m-1}a_{m-2}a_{m-3}\ldots a_1a_0) = (000\ldots00)$

- Rovnice vyjadřuje tzv. aditivní identitu.
- Odčítání se definováno jako přičítání aditivní inverze.
- Protože platí aditivní identita jsou operace sčítání a odčítání nad F_2^m ekvivalentní.

Závěr: Sčítání i odčítání se realizuje operací XOR

EC nad konečným polem typu F_2^m

- Při násobení polynomů stupně nižšího než *m* může vzniknout polynom stupně vyššího než *m*
- Redukční (nedělitelný) polynom f(*x*) stupně m pomocí operace mod f(x) zajistí, že výsledek operací bude ležet v F_2^m
- V kryptografii se využívají:
  - trinomiály ve tvaru $x^m + x^k + 1,\ 1 \leq k \leq m\text{-}1$
  - pentomiály ve $x^m + x^a + x^b + x^c + 1$, kde $1 \leq c < b < a \leq m - 1$

- Redukční polynom f(*x*) je každý polynom, který odpovídá triominálnímu nebo pentominálnímu tvaru a pro který platí, že je nad polem F_2^m nerozložitelný, tj. nelze ho vyjádřit jako součin dvou polynomů o stupni nižším než m

EC nad konečným polem typu F_2^m

Pravidla pro aritmetické operace v F_2^m mohou být definovány dvěma způsoby.

Můžeme vyjít z reprezentace

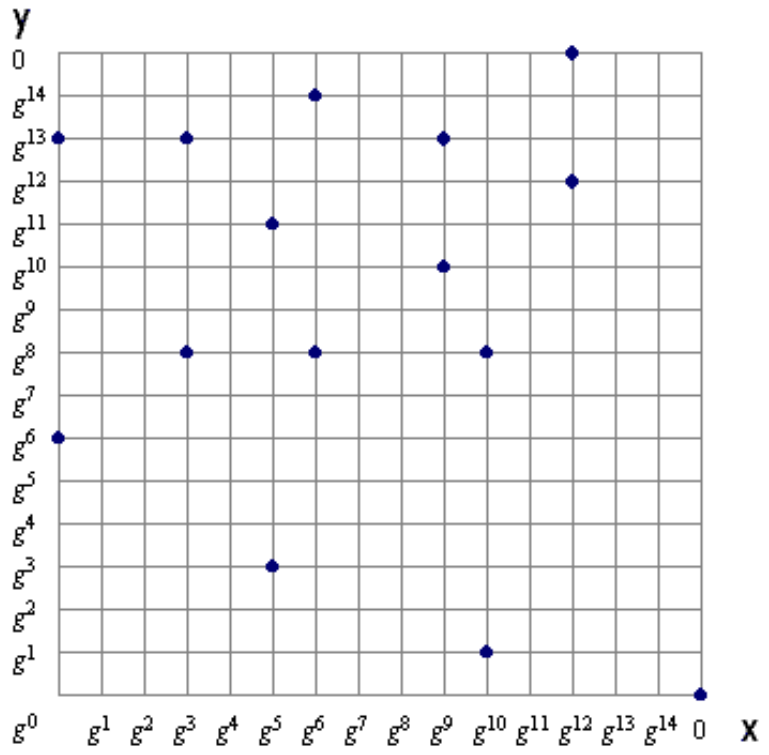
- **polynomiální bází**
  není tak efektivní jako ONB
- **optimální normální bází (ONB)**
  velmi efektivní
  nevhodné pro pochopení principů…

Hlavní rozdíl spočívá v definici násobení mezi prvky pole.

EC nad konečným polem typu F_2^m - PŘÍKLAD

Ukázka eliptické křivky nad polem F_2^4 s polynomiální reprezentací popsaná rovnicí $y^2 + xy = y^3 + g^4 x^2 + g^0$

Pro jednodušší zápis jsou souřadnice bodů zapisovány s využitím generátoru.



EC nad konečným polem typu F_2^m

- Grupy na eliptických křivkách nad F_2^m mají konečný počet bodů a aritmetické operace s nimi nevykazují žádné zaokrouhlovací chyby.

- Tyto vlastnosti spojené s binární povahou pole vedou k tomu, že početní operace mohou být velmi efektivně implementovány počítačem.

Doménové parametry pro EC

- kromě parametrů *a,b* se komunikující strany musí dohodnout na dalších parametrech
- doménové (systémové) parametry
- různé pro F_p a F_2^m
- volba parametrů popsána v doporučení:
  Standards for Efficient Cryptography, *SEC 2: Recommended Elliptic Curve Domain Parameters, Version 1.0, September 2000,* http://www.secg.org/download/aid-386/sec2_final.pdf

Doménové parametry pro EC nad poli typu F_p

- **p** – prvočíslo definující podložní pole F_p
- **a,b** – parametry definující konkrétní eliptickou křivku ve tvaru $y^2 \bmod p = x^3 + ax + b \bmod p$
- **g** – generátor; bod (x_g, y_g) ležící na EC
- **n** – řád křivky
- **h** – kofaktor $h = \frac{\#E(F_p)}{n}$

$\#E(F_p)$ … počet bodů EC sestrojené nad polem F_p

Typické hodnoty pro EC typu F_p a F_{2^m}

- SW implementace …spíše křivky nad poli typu F_p
  - $p = 2^{192} - 2^{64} - 1$
  - $p = 2^{192} - 2^{64} - 1$
  - $p = 2^{224} - 2^{96} - 1$
  - $p = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$
  - $p = 2^{384} - 2^{128} - 2^{96} + 2^{32} - 1$
  - $p = 2^{521} - 1$
- HW implementace …spíše křivky nad poli typu F_{2^m}
  - m = 163
  - m = 233
  - m = 283
  - m = 409
  - m = 571

Doménové parametry pro EC nad poli typu F_2^m

- **m** – řád pole, celé číslo definující konečné binární pole F_2^m
- **f(x)** – nedělitelný polynom stupně ***m***
- **a, b** – parametry definující konkrétní EC ve tvaru

$$y^2 + xy = x^3 + ax^2 + b$$

- **g** – generátor v poli F_2^m ;bod (x_g, y_g) ležící na EC
- **n** – řád křivky (při násobení se násobí číslem <0;n-1>
- **h** - kofaktor $h = \frac{\#E(F_{2^m})}{n}$

Problém diskrétního logaritmu na EC

Praktické kryptografické algoritmy využívající EC jsou postaveny na nemožnosti řešení ECDLP problému

Definice ECDLP: Mějme eliptickou křivku E řádu n definovanou nad polem F_p a bod Q ležící na E.

Určete celé číslo k takové, že $Q=k \cdot P$, $0 \leq k \leq n-1$

Číslo k je diskrétní logaritmus Q o základu P na křivce E.

V kryptosystémech je Q veřejný klíč a k soukromý klíč.

*V*elikost ***k*** musí zabránit výpočtu diskrétního logaritmu postupným násobením.

Problém diskrétního logaritmu na EC

- ECDLP je efektivně neřešitelný
- Pro danou velikost pole (typicky pole F_2^{160} ….. 2^{160} prvků) je nesmírně obtížné zjistit *k* ze znalosti dvojice *k*·*P* a *P*.

- O problému ECDLP se předpokládá, že je odolný vůči útokům typu NFS (Number Field Sieve).

- Dnes neefektivnějším známým útokem je Pollardova ρ-metoda se složitostí přibližně $O\left(\frac{\sqrt{\pi n}}{2}\right)$ kroků, kde *n* je počet prvků pole.

IEEE P1363

3úrovňový model k rozlišení různých typů kryptografických technik:

- kryptografická primitiva
  - základní matematické operace
  - stavební prvek pro schémata
  - samo o sobě nedokáže zajistit bezpečnost
- kryptografická schémata
  - kombinuje kryptografická primitiva a další doplňkové operace
  - schéma může zajistit bezpečnost (v k. protokolu)
- kryptografické protokoly
  - při správné aplikace protokoly mohou dosáhnout požadované bezpečnosti
  - posloupnost kroků (pravidel) pro komunikaci dvou nebo více stran s nějakým (bezpečnostním) cílem

IEEE P1363 - primitiva

- SVDP – Secret Value Derivation Primitive
  - odvození tajné hodnoty ve schématech pro výměnu klíčů (např. DLSVDP-DH)
- SP/VP – Signature/Verification Primitive
  - generování/ověření podpisu ve schématech řešících eln. podpis (např. ECSP-DSA, IFSP-RSA1)
- EP/DP – Encryption/Decryption Primitive
  - šifrování/dešifrování v šifrovacích schématech (např. IFDP-RSA)

IEEE P1363 - schémata

- KAS – Key Agreement Scheme
  - komunikující strany vytvoří sdílený tajný klíč s využitím svých klíčových párů
- SSA – Signature Scheme with Appendix
  - jedna strana podepíše zprávu, druhá ji může ověřit
  - podpis není součástí zprávy
- SSR – Signature Scheme with Message Recovery
  - jedna strana podepíše zprávu, druhá ji může ověřit
  - zpráva je odkryta pouze v případě verifikace podpisu
  - podpis není oddělen od zprávy
- ES – Encryption Scheme
  - jedna ze stran zašifruje zprávu veřejným klíčem příjemce
  - lze využít k dohodě na tajném klíči pro symetrické kryptosystémy

Algoritmy využívající EC

- vybrané algoritmy využívající EC
  - ECDSA
  - ECDH
  - ECIES
  - ECMQV

ECDSA (Elliptic Curve Digital Signature Algorithm)

ECDSA slouží k podepisování a ověřování podpisu
- nelze jej použít k šifrování
- analogický k DSA
- standardizován v normách FIPS 186-2, ANSI X9.62, IEEE P1363 a ISO/IEC 15946-2
- první standardizovaný algoritmus využívající EC

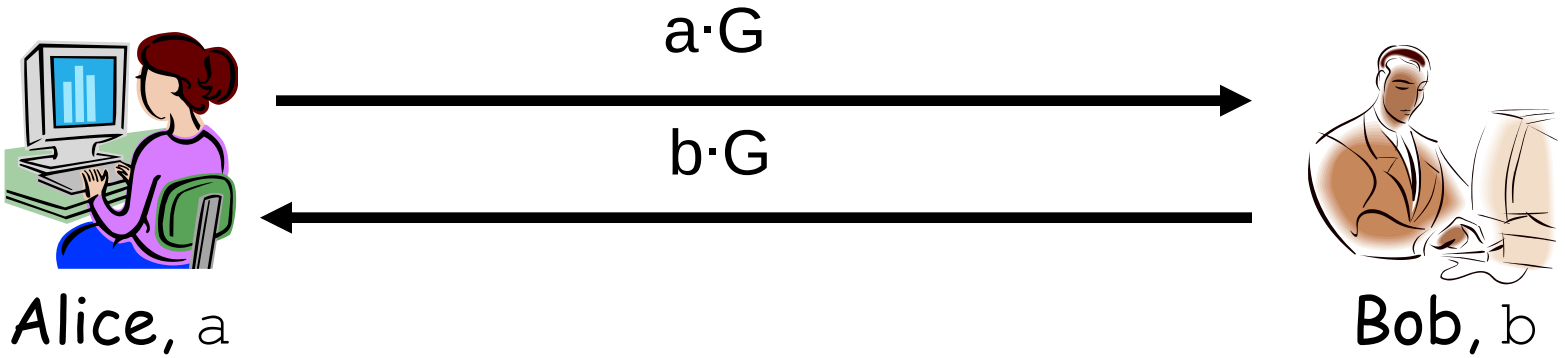
3 základní kroky
- generování klíče
- generování podpisu
- ověření podpisu

ECDH (Elliptic Curve Diffie-Hellman)

- algoritmus analogický s klasickým Diffieellmanovým algoritmem
- umožňuje komunikujícím stranám získat sdílenou tajnou informaci použitelnou např. jako klíč pro klasickou symetrickou šifru

ECDH (Elliptic Curve Diffie-Hellman)

- **Veřejný klíč:** G (bod na eliptické křivce)
- **Tajný klíč:** pro Alici číslo a, pro Boba číslo b



- Alice spočítá $a \cdot (b \cdot G)$
- Bob spočítá $b \cdot (a \cdot G)$
- $K = a \cdot (b \cdot G) = b \cdot (a \cdot G)$ je možné použít jako klíč pro symetrickou šifru; K – souřadnice jiného bodu na křivce
- potencionální útočník může zachytit pouze G,aG, bG

El-Gamal pomocí ECDLP

Účastníci *A* a *B* se dohodnou na parametrech křivky *E*.
Účastník *A* si zvolí bod *X* na křivce *E*.
Účastník *A* si dále zvolí číslo *s* (tajný klíč) a spočte *X= sP (veřejný klíč)*.
Účastník *A* předá účastníkovi *B* souřadnice bodu *P* a číslo *X*.

Aby účastník *B* mohl poslat šifrovanou zprávu účastníkovi *A*, musí:

- vyjádřit svou zprávu jako bod *M* na křivce *E*
- zvolit náhodné číslo *k* a spočítat
  - $M_1=kP$
  - $M_2=M+kX$
- odeslat M_1 a M_2 účastníkovi *B*

Účastník *B* dešifruje zprávu $M = M_2 – sM_1$
Funguje to protože:

$$M_2 – sM_1=(M+ kX) – s(kP) = M + k(sP) – skP = M$$

Elliptic Curve Integrated Encryption Scheme

- ECIES - šifrovací schéma využívající EC
- strana, která začíná komunikaci pomocí ECDH získá tajnou informaci, ze které se vygeneruje klíč, který je pak použit k šifrování nebo podepisování.
  - představen v roce 1998 (Abdalla, Bellare a Rogaway)
  - varianta ElGamalova schématu
  - obsažen v standardech ANSI X9.63, ISO/IEC 15946-3 a IEEE 1363

ECMQV - Elliptic Curve Menezes-Qu-Vanstone

- výměna klíčů pomocí EC odvozená z DH schématu
- měl být bezpečnější než ECDH
- patentován firmou Certicom
- NSA zaplatila 25 mil. $ aby ho mohla použít v „Suite B“
  - ECMQV byl mezi algoritmy zmiňované v „Suite B“ od NSA
  - aktuálně vyřazen ze Suite B kvůli bezpečnostním problémům
- standardizován v ANSI X9.63, ISO/IEC 15946-3 a IEEE P1363

Srovnání s ostatními kryptosystémy

Základní srovnávací hlediska:

Efektivita

- **Výpočetní režie** - počet výpočetních operací nutných k šifrování a dešifrování
- **Velikost klíče nebo podpisu** - jaký objem (počet bitů) zabírají veřejný a soukromý klíč a systémové parametry
- **Šířka pásma** - jaký objem dat je nutný k přenesení zašifrované zprávy nebo podpisu

Bezpečnost – který z problémů je těžší ?

IFP x **DLP** x **ECDLP**

Efektivita – výpočetní režie

ECC jsou při šifrování zhruba

- 10x rychlejší než IFP(RSA) a DLP (DSA) algoritmy
- použití krátkého veřejného exponentu urychlí RSA na úroveň ECC
- krátký veřejný exponent RSA nemá vliv na dobu dešifrování nebo generování podpisu

Efektivita – velikosti klíčů a systémových parametrů

Srovnání kryptosystémů se srovnatelnou úrovní zabezpečení

- Systémové parametry u IFP(RSA) nejsou
- Systémové parametry u ECC jsou: pole F_p, dva koeficienty a,b určující křivku, generátor G ležící na EC a řád generátoru n.
- Systémové parametry u DSA jsou: prvočíslo q, prvočíslo p takové že q dělí $p-1$, generátor g.

Algoritmus	Systémové parametry [b]	Veřejný klíč [b]	Soukromý klíč [b]
RSA	n/a	1088*	2048*
DSA	2208	1024	160
ECC	481	161	160

* modul + veřejný/tajný exponent (veřejný zvolen krátký kvůli urychlení)

Efektivita – šířka pásma

- stejné nároky na šířku pásma při šifrování nebo podepisování dlouhých zpráv
- kryptosystémy veřejného klíče se často využívají k přenosu krátkých zpráv
- pro krátké zprávy má kryptosystém na bázi EC menší nároky na šířku pásma než ostatní systémy veřejného klíče

Algoritmus	Velikost podpisu [b]
RSA	1024
DSA	320
ECDSA	320

velikost digitálního podpisu, OT= 2kb

Algoritmus	Délka zašifrované zprávy [b]
RSA	1024
El-Gamal[1]	2048
ECES	321

velikost zašifrované zprávy, OT=100b

[1] DSA slouží pouze k digitálnímu podpisu, proto byl k šifrování použit systém El-Gamal, jehož bezpečnost stejně jako bezpečnost DSA spočívá v obtížnosti řešení výpočtu diskrétního logaritmu.

Bezpečnost – srovnání IFP, DLP a ECDLP

IFP

- **Pollardova** ρ, p-1, p+1 metoda
- **NFS** (Number Field Sieve)
- **TWINKLE, TWIRL** (zatím jen teoretické návrhy)
  - optická zařízení urychlující (100-1000x) počáteční fázi prohledávání možných řešení. Po skončení se pokračuje s klasickým NFS. Stroj v ceně několika desítek miliónů dolarů umožní prolomení jednoho klíče RSA s délkou modulu 1024 bitů za 1 rok.
- kvantové počítače (zatím jen teoreticky)
  - podařilo se sestrojit KP, který faktorizoval číslo 15

Bezpečnost – srovnání IFP, DLP a ECDLP

DLP

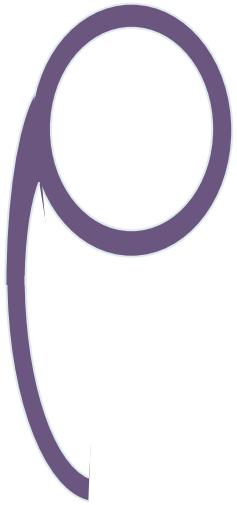
Obdobné metody jako u kryptosystémů na bázi IFP a navíc několik specifických útoků na DLP:

- Index-Calculus
- Pollardova ρ a λ metoda pro DL
- Pohlingův-Hellmanův algoritmus

Bezpečnost – srovnání IFP, DLP a ECDLP

ECDLP

- nejefektivnější známá metoda – Pollardova ρ
- časová složitost $O(\sqrt{\frac{\pi n}{2}})$ kroků (n je typicky 2^{160} a více !!!)
- výhoda - malá pamětová složitost
- lze paralelizovat – při použití *m* strojů je složitost $O(\frac{\sqrt{\frac{\pi n}{2}}}{m})$



Bezpečnost – srovnání IFP, DLP a ECDLP

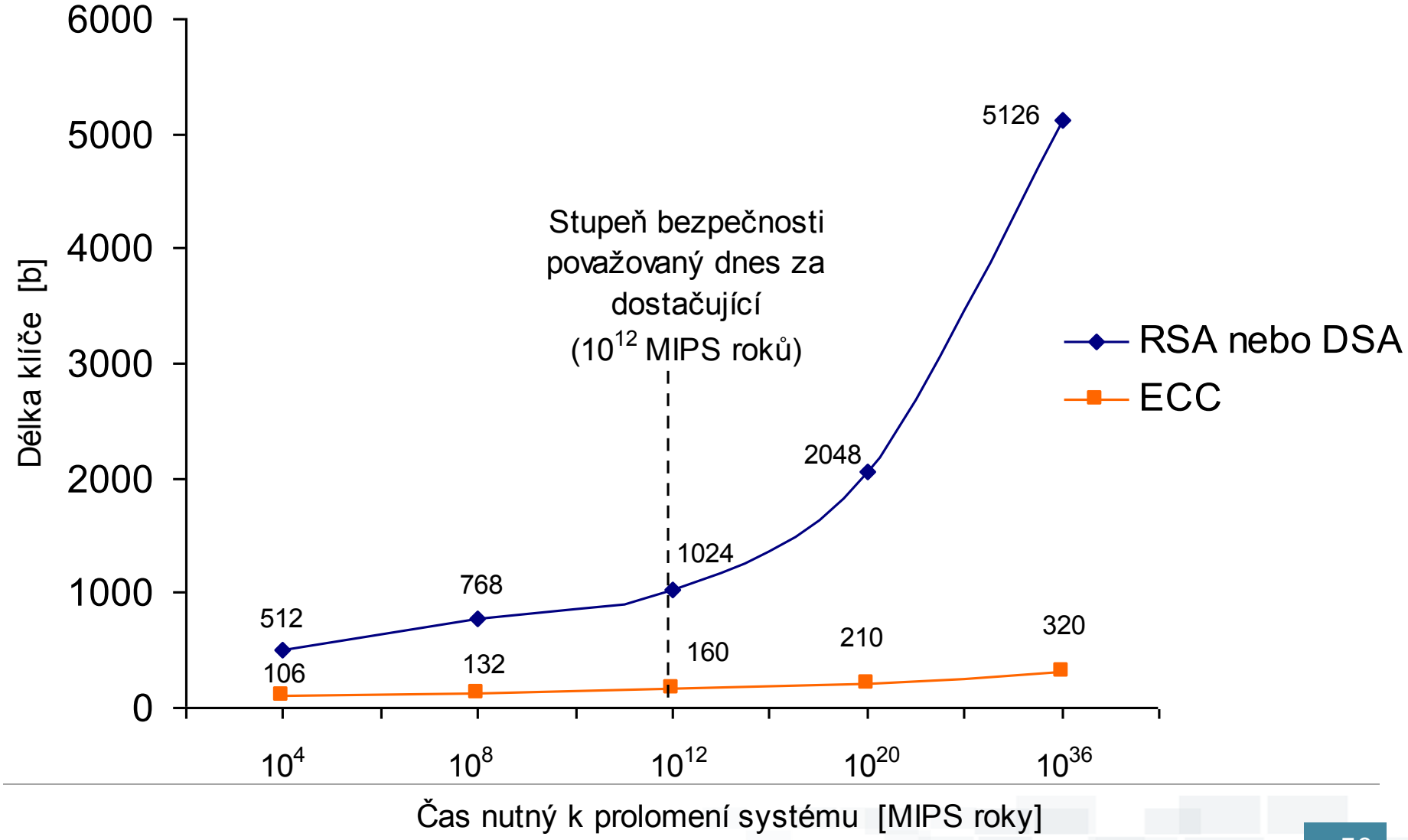
- Pro speciální třídy křivek - supersingulární
  - anomální

  lze problém ECDLP převést na DLP a pro něj existují „rychlé“ algoritmy (řešitelné v sub-exponenciálním čase)

- Použití těchto typů křivek je v příslušných doporučeních zakázáno.

- Pro obecné EC dnes nejsou známy žádné algoritmy s subexponenciální časovou složitostí, nejlepší algoritmy mají plně exponenciální složitost.
- V současné době ECDLP podstatně obtížněji řešitelný než DLP.

Bezpečnost – srovnání IFP, DLP a ECDLP



Bezpečnost – srovnání IFP, DLP a ECDLP

Srovnání růstu velikosti klíčů u ECC a RSA (DSA) při ekvivalentní úrovni bezpečnosti

Čas nutný k prolomení [MIPS roky]	RSA (DSA) velikost klíče [b]	ECC velikost klíče [b]	RSA/ECC poměr velikosti klíčů
10^4	**512**	**106**	**5 : 1**
10^8	**768**	**132**	**6 : 1**
10^{11}	**1,024**	**160**	**7 : 1**
10^{20}	**2,048**	**210**	**10 : 1**
10^{78}	**21,000**	**600**	**35 : 1**

Srovnatelná bezpečnost různých typů kryptosystémů pro různé délky klíčů [b]

Symetrické šifry	ECDLP	IFP/DLP	Bezpečnost
56	112	512	**NEBEZPEČNÉ** - dnes již dokážeme luštit
64	128	768	**Krátkodobá bezpečnost** (do 5-10 letech půjde luštit; jsou publikovány úspěšné pokusy o prolomení)
80	163	1024	**Dlouhodobá bezpečnost** - pokud nedojde k novým zásadním objevům nebo konstrukci kvantového počítače
112	231	2048	
128	283	3072	
192	409	7680	
256	571	15360	

Největší EC, pro které se povedl vyřešit ECDLP

Délka [b]	Typ [Prime/Binary]	Vyřešeno
79	Prime	12/1997
79	Binary	12/1997
89	Prime	01/1998
89	Binary	02/1998
97	Prime	03/1998
95	Binary	05/1998
97	Binary	09/1999
108	Binary	04/2000
109	Prime	11/2002
109	Binary	4/2004
131	P/B	?

Suite B – co to je

- „doporučení“ pro bezpečné sdílení informací v mezinárodním měřítku z dílny NSA, NIST a NATO
- Suite-B algoritmy jsou určeny pro šifrování klasifikovaných informací*, ale samotné algoritmy nejsou tajné a jsou volně dostupné
- publikován 16.3.2005
- obsahuje tři základní komponenty:
  - asymetrické algoritmy na bázi ECC
  - symetrický algoritmus AES
  - hashovací funkce z rodiny SHA-2

http://www.nsa.gov/ia/industry/crypto_suite_b.cfm

* Confidental, Secret, TopSecret

Suite B – co to je

- NIST definoval několik množin EC z nichž nejdůležitější jsou ty které generuje rovnice

$$Y^2 = x^3 - 3x + b \pmod{p}$$

- Tři nejdůležitější křivky z podložního pole F_p jsou:
  - P-256, s délkou modulu 256 bitů, (bezpečnost je ekvivalentní s AES-128)
  - P-384, s délkou modulu 384 bitů, (bezpečnost je ekvivalentní s AES-192)
  - P-512, s délkou modulu 512 bitů, (bezpečnost je ekvivalentní s AES-256)

- Tyto tři křivky tvoří základ algoritmů skupiny „Suite B“

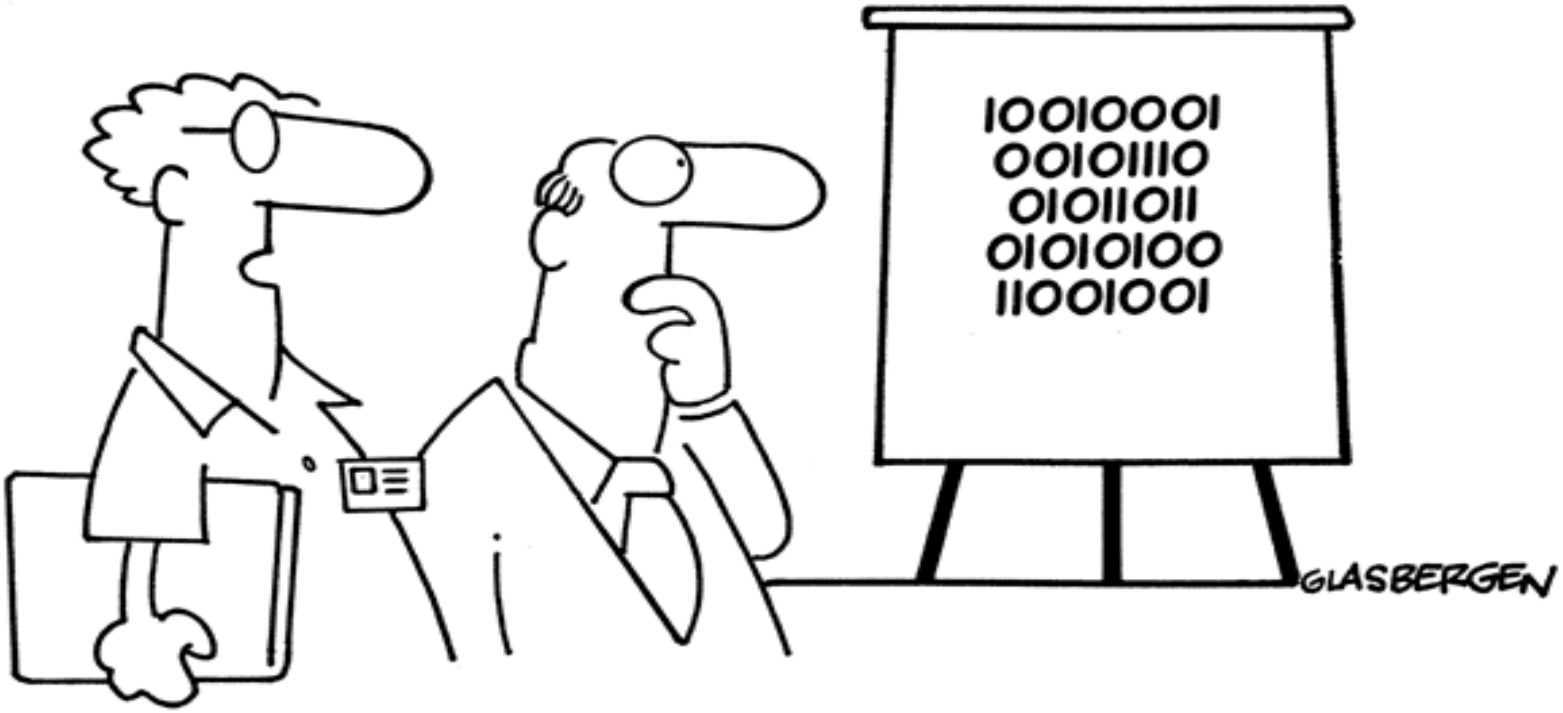
Suite B – algoritmy

- Šifrování - AES (FIPS 197)
  - AES-128 až do úrovně SECRET
  - AES-256 až do úrovně TOP SECRET
- Elektronický podpis (FIPS 186-3)
  - ECDSA s prvočísleným modulem délky 256 bitů až do úrovně SECRET
  - ECDSA s prvočísleným modulem délky 384 bitů až do úrovně TOP SECRET
- Výměna klíčů (NIST SP 800-56A)
  - ECDH s prvočísleným modulem délky 256 bitů až do úrovně SECRET
  - ECDH s prvočísleným modulem délky 384 bitů až do úrovně až do úrovně TOP SECRET
- Hashovací funkce (FIPS 180-2)
  - SHA-256 do úrovně SECRET
  - SHA-384 do úrovně TOP SECRET

Suite A

- existuje i sada „Suite A“
- množina neveřejných algoritmů
- obsahuje algoritmy (kategorie Type-1) vyvinuté nebo certifikované NSA pro šifrování klasifikovaných informací:
  - ACCORDION
  - BATON - symetrická šifra s délkou bloku 128 bitů a délkou klíče 320 bitů; 160 bitů klíče je použito k zajištění integrity
  - MEDLEY
  - SHILLELAGH
  - WALBURN

O těchto algoritmech není známo takřka nic (kromě toho, že existují).



"We've devised a new security encryption code. Each digit is printed upside down."

- IEEE P1363: Standard Specifications for Public Key Cryptography
- ANSI X9.62: The Elliptic Curve Digital Signature Algorithm
- ANSI X9.63: Key Agreement and Key Management Using ECC
- PKCS #13: Elliptic Curve Cryptography Standard
- Internet X.509 Public Key Infrastructure Representation of ECDSA Keys and Signatures in Internet X.509 Public Key Infrastructure Certificates,
- ISO/IEC 15946 Information technology - Security techniques - Cryptographic techniques based on elliptic curves

Dotazy