Bezpečnost mobilních telefonů

úvod do kryptologie

David Machač

FJFI ČVUT v Praze

NMT

- Nordic Mobile Telephony, 1981
- analogová síť
- u nás: 1991 - 1996
- ŽÁDNÉ šifrování
- výhoda: pokrytí

Obrázek: Nokia Mobira Cityman (1987)

NMT

- Nordic Mobile Telephony, 1981
- analogová síť
- u nás: 1991 - 1996
- ŽÁDNÉ šifrování
- výhoda: pokrytí

Obrázek: Nokia Mobira Cityman (1987)

NMT

- Nordic Mobile Telephony, 1981
- analogová síť
- u nás: 1991 - 1996
- ŽÁDNÉ šifrování
- výhoda: pokrytí

Obrázek: Nokia Mobira Cityman (1987)

NMT

- Nordic Mobile Telephony, 1981
- analogová síť
- u nás: 1991 - 1996
- ŽÁDNÉ šifrování
- výhoda: pokrytí

Obrázek: Nokia Mobira Cityman (1987)

NMT

- Nordic Mobile Telephony, 1981
- analogová síť
- u nás: 1991 - 1996
- ŽÁDNÉ šifrování
- výhoda: pokrytí

Obrázek: Nokia Mobira Cityman (1987)

GSM

- Global System for Mobile Communications, 1991
- digitální
- šifrovaná
- algoritmy A5/1, A5/2

GSM

- Global System for Mobile Communications, 1991
- digitální
- šifrovaná
- algoritmy A5/1, A5/2

GSM

- Global System for Mobile Communications, 1991
- digitální
- šifrovaná
- algoritmy A5/1, A5/2

GSM

- Global System for Mobile Communications, 1991
- digitální
- šifrovaná
- algoritmy A5/1, A5/2

A5/1

- vyvinuta 1987, unikla 1994
- proudová šifra
- kombinace tří registrů
- linear feedback shift register (LFSR)

A5/1

- vyvinuta 1987, unikla 1994
- proudová šifra
- kombinace tří registrů
- linear feedback shift register (LFSR)

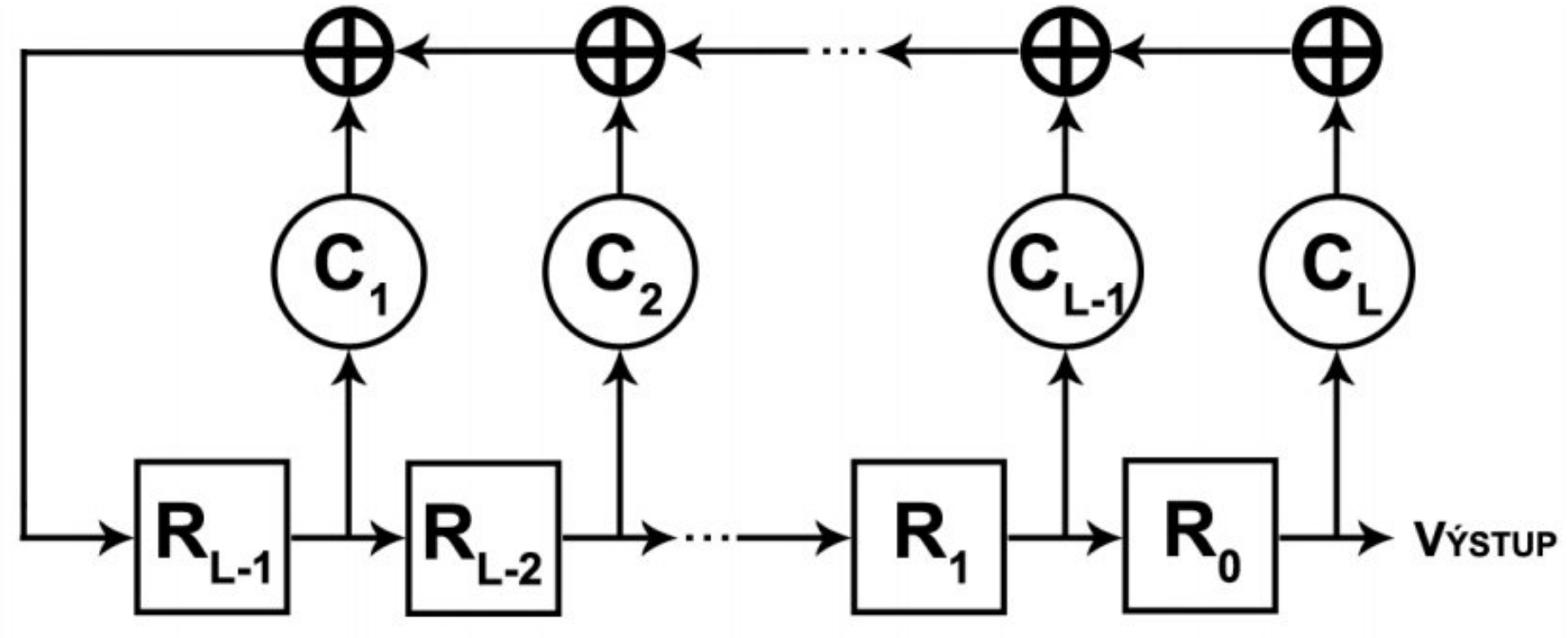
A5/1

- vyvinuta 1987, unikla 1994
- proudová šifra
- kombinace tří registrů
- linear feedback shift register (LFSR)

A5/1

- vyvinuta 1987, unikla 1994
- proudová šifra
- kombinace tří registrů
- linear feedback shift register (LFSR)

A5/1



Obrázek: LFSR

A5/1

- GSM přenos probíhá dávkově
- 114 bitů každých 4,615 ms (upstream)
- v každém taktu jsou pozorovány taktovací bity
- zjišťen většinový bit
- $\Rightarrow$ posun 2 registrů, každý se posune s pravděpodobností 3/4

č. LFSR	délka [b]	char. pol	taktovací bit
1.	19	$x^{18} + x^{17} + x^{16} + x^{13} + 1$	8
2.	22	$x^{21} + x^{20} + 1$	10
3.	23	$x^{22} + x^{21} + x^{20} + x^{7} + 1$	10

Tabulka: parametry LFSR pro A5/1

A5/1

- GSM přenos probíhá dávkově
- 114 bitů každých 4,615 ms (upstream)
- v každém taktu jsou pozorovány taktovací bity
- zjišťen většinový bit
- $\Rightarrow$ posun 2 registrů, každý se posune s pravděpodobností 3/4

č. LFSR	délka [b]	char. pol	taktovací bit
1.	19	$x^{18} + x^{17} + x^{16} + x^{13} + 1$	8
2.	22	$x^{21} + x^{20} + 1$	10
3.	23	$x^{22} + x^{21} + x^{20} + x^{7} + 1$	10

Tabulka: parametry LFSR pro A5/1

A5/1

- GSM přenos probíhá dávkově
- 114 bitů každých 4,615 ms (upstream)
- v každém taktu jsou pozorovány taktovací bity
- zjišťen většinový bit
- $\Rightarrow$ posun 2 registrů, každý se posune s pravděpodobností 3/4

č. LFSR	délka [b]	char. pol	taktovací bit
1.	19	$x^{18} + x^{17} + x^{16} + x^{13} + 1$	8
2.	22	$x^{21} + x^{20} + 1$	10
3.	23	$x^{22} + x^{21} + x^{20} + x^{7} + 1$	10

Tabulka: parametry LFSR pro A5/1

A5/1

- GSM přenos probíhá dávkově
- 114 bitů každých 4,615 ms (upstream)
- v každém taktu jsou pozorovány taktovací bity
- zjišťen většinový bit
- $\Rightarrow$ posun 2 registrů, každý se posune s pravděpodobností 3/4

č. LFSR	délka [b]	char. pol	taktovací bit
1.	19	$x^{18} + x^{17} + x^{16} + x^{13} + 1$	8
2.	22	$x^{21} + x^{20} + 1$	10
3.	23	$x^{22} + x^{21} + x^{20} + x^{7} + 1$	10

Tabulka: parametry LFSR pro A5/1

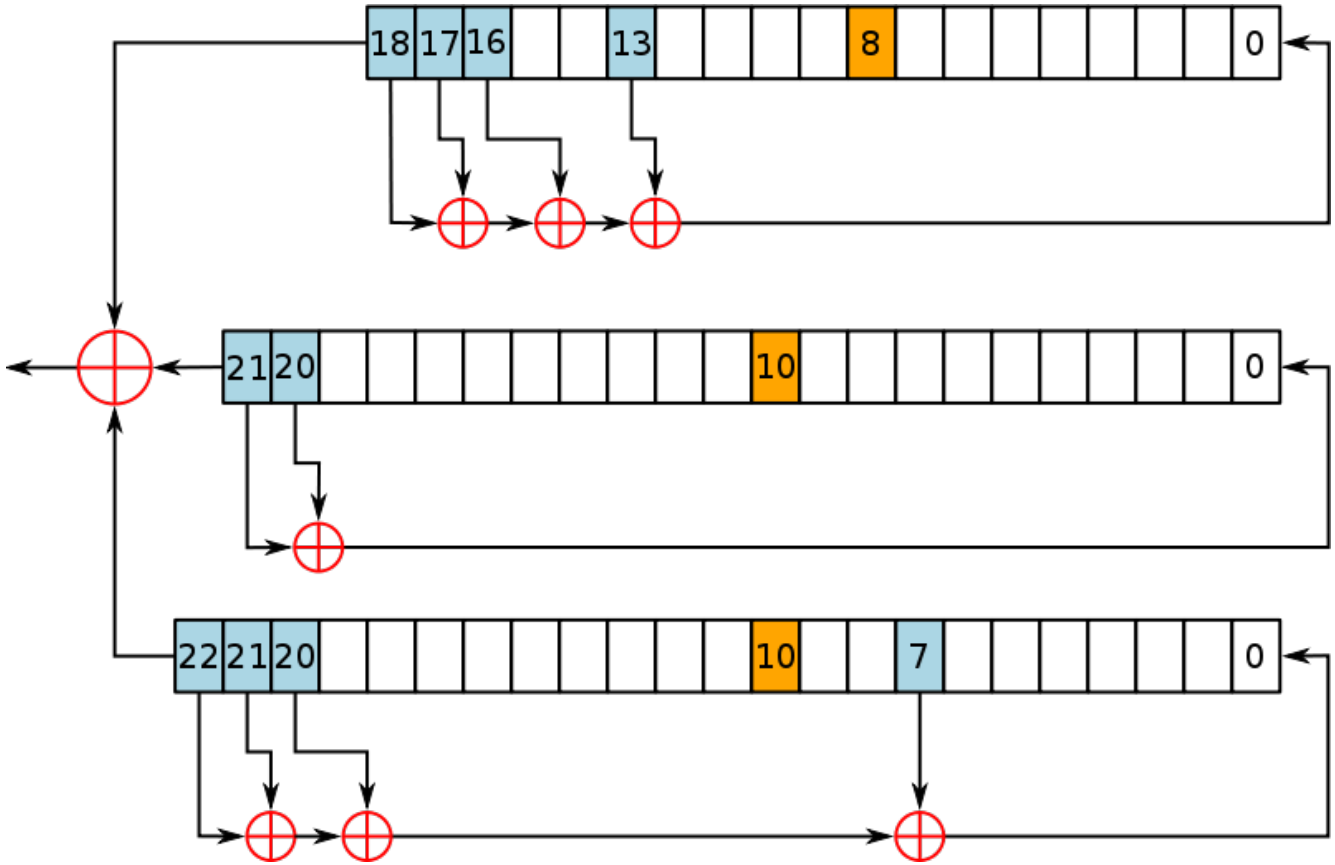
A5/1

- GSM přenos probíhá dávkově
- 114 bitů každých 4,615 ms (upstream)
- v každém taktu jsou pozorovány taktovací bity
- zjišťen většinový bit
- $\Rightarrow$ posun 2 registrů, každý se posune s pravděpodobností 3/4

č. LFSR	délka [b]	char. pol	taktovací bit
1.	19	$x^{18} + x^{17} + x^{16} + x^{13} + 1$	8
2.	22	$x^{21} + x^{20} + 1$	10
3.	23	$x^{22} + x^{21} + x^{20} + x^{7} + 1$	10

Tabulka: parametry LFSR pro A5/1

A5/1



Obrázek: LFSR pro A5/1

A5/1

- na počátku jsou všechny registry nastaveny na 0
- poté:

for $i := 1$ to 64 **do**
  $R[0] := R[0] \oplus K[i]$
  shift
end for

- K je tajný klíč
- taktování je provedeno 100x
- výhoda: snadná hardwarová implementace

A5/1

- na počátku jsou všechny registry nastaveny na 0
- poté:

  for $i := 1$ to 64 **do**
  $R[0] := R[0] \oplus K[i]$
  shift
  end for

- K je tajný klíč
- taktování je provedeno 100x
- výhoda: snadná hardwarová implementace

A5/1

- na počátku jsou všechny registry nastaveny na 0
- poté:

  for $i := 1$ to 64 **do**
    $R[0] := R[0] \oplus K[i]$
    shift
  end for

- K je tajný klíč
- taktování je provedeno 100x
- výhoda: snadná hardwarová implementace

A5/1

- na počátku jsou všechny registry nastaveny na 0
- poté:

  for $i := 1$ to 64 **do**
  $R[0] := R[0] \oplus K[i]$
  shift
  end for

- K je tajný klíč
- taktování je provedeno 100x
- výhoda: snadná hardwarová implementace

A5/1

- na počátku jsou všechny registry nastaveny na 0
- poté:

  for $i := 1$ to 64 **do**
  $R[0] := R[0] \oplus K[i]$
  shift
  end for

- K je tajný klíč
- taktování je provedeno 100x
- výhoda: snadná hardwarová implementace

A5/1

- na počátku jsou všechny registry nastaveny na 0
- poté:

  for $i := 1$ to 64 **do**
  $R[0] := R[0] \oplus K[i]$
  shift
  end for

- K je tajný klíč
- taktování je provedeno 100x
- výhoda: snadná hardwarová implementace

A5/1

- na počátku jsou všechny registry nastaveny na 0
- poté:

  for $i := 1$ to 64 **do**
  $R[0] := R[0] \oplus K[i]$
  shift
  end for

- K je tajný klíč
- taktování je provedeno 100x
- výhoda: snadná hardwarová implementace

A5/1

- na počátku jsou všechny registry nastaveny na 0
- poté:

  for $i := 1$ to 64 **do**
  $R[0] := R[0] \oplus K[i]$
  shift
  end for

- K je tajný klíč
- taktování je provedeno 100x
- výhoda: snadná hardwarová implementace

A5/1

- na počátku jsou všechny registry nastaveny na 0
- poté:

  for $i := 1$ to 64 **do**
  $R[0] := R[0] \oplus K[i]$
  shift
  end for

- K je tajný klíč
- taktování je provedeno 100x
- výhoda: snadná hardwarová implementace

prolomení A5/1 na základě znalosti šif. a nešif. textu

- 1997 (Golic) - řešení soustavy lineárních rovnic, složitost $2^{40,16}$
- 2000 (Biryukov, Shamir, Wagner) - memory tradeoff attack - snížím nároky na výpočetní výkon na úkor vyšší spotřeby paměti - zjištění klíče do dvou minut, avšak předtím je zapotřebí provést 2^{48} operací k získání $\pm$ 300 GB dat
- 2000 (Biham, Dunkelman) - složitost $2^{39,91}$ při znalosti $2^{20,8}$ bitů plaintextu, vyžaduje 32 GB dat + 2^{38} kroků k jejich získání
- 2004 (Ekdahl, Johanson) - prolomení během „pár minut“ se znalostí $\pm 2^{21}$ plaintextu

prolomení A5/1 na základě znalosti šif. a nešif. textu

- 1997 (Golic) - řešení soustavy lineárních rovnic, složitost $2^{40,16}$
- 2000 (Biryukov, Shamir, Wagner) - memory tradeoff attack - snížím nároky na výpočetní výkon na úkor vyšší spotřeby paměti - zjištění klíče do dvou minut, avšak předtím je zapotřebí provést 2^{48} operací k získání $\pm$ 300 GB dat
- 2000 (Biham, Dunkelman) - složitost $2^{39,91}$ při znalosti $2^{20,8}$ bitů plaintextu, vyžaduje 32 GB dat + 2^{38} kroků k jejich získání
- 2004 (Ekdahl, Johanson) - prolomení během „pár minut“ se znalostí $\pm 2^{21}$ plaintextu

prolomení A5/1 na základě znalosti šif. a nešif. textu

- 1997 (Golic) - řešení soustavy lineárních rovnic, složitost $2^{40,16}$
- 2000 (Biryukov, Shamir, Wagner) - memory tradeoff attack - snížím nároky na výpočetní výkon na úkor vyšší spotřeby paměti - zjištění klíče do dvou minut, avšak předtím je zapotřebí provést 2^{48} operací k získání $\pm$ 300 GB dat
- 2000 (Biham, Dunkelman) - složitost $2^{39,91}$ při znalosti $2^{20,8}$ bitů plaintextu, vyžaduje 32 GB dat + 2^{38} kroků k jejich získání
- 2004 (Ekdahl, Johanson) - prolomení během „pár minut“ se znalostí $\pm 2^{21}$ plaintextu

prolomení A5/1 na základě znalosti šif. a nešif. textu

- 1997 (Golic) - řešení soustavy lineárních rovnic, složitost $2^{40,16}$
- 2000 (Biryukov, Shamir, Wagner) - memory tradeoff attack - snížím nároky na výpočetní výkon na úkor vyšší spotřeby paměti - zjištění klíče do dvou minut, avšak předtím je zapotřebí provést 2^{48} operací k získání $\pm$ 300 GB dat
- 2000 (Biham, Dunkelman) - složitost $2^{39,91}$ při znalosti $2^{20,8}$ bitů plaintextu, vyžaduje 32 GB dat + 2^{38} kroků k jejich získání
- 2004 (Ekdahl, Johanson) - prolomení během „pár minut“ se znalostí $\pm 2^{21}$ plaintextu

prolomení A5/1 na základě znalosti pouze šif. textu (v GSM)

- 2003 (Barkan a kol.) - donucení telefonu k dočasnému použití slabší šifry A5/2, a z ní zjištění klíče (stejný pro A5/1)
- 2008 (skupina Hackers Choice) - projekt, který umožňuje po 3-5 minutách odhalit klíč (s využitím 3 TB tabulky)
- podobný projekt - univerzity v Bochumi a Kielu

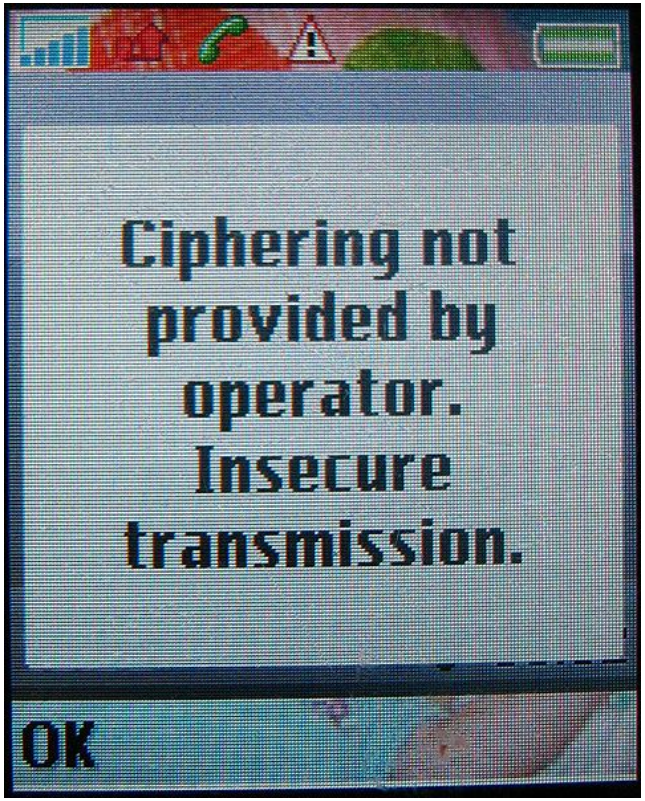
prolomení A5/1 na základě znalosti pouze šif. textu (v GSM)

- 2003 (Barkan a kol.) - donucení telefonu k dočasnému použití slabší šifry A5/2, a z ní zjištění klíče (stejný pro A5/1)
- 2008 (skupina Hackers Choice) - projekt, který umožňuje po 3-5 minutách odhalit klíč (s využitím 3 TB tabulky)
- podobný projekt - univerzity v Bochumi a Kielu

prolomení A5/1 na základě znalosti pouze šif. textu (v GSM)

- 2003 (Barkan a kol.) - donucení telefonu k dočasnému použití slabší šifry A5/2, a z ní zjištění klíče (stejný pro A5/1)
- 2008 (skupina Hackers Choice) - projekt, který umožňuje po 3-5 minutách odhalit klíč (s využitím 3 TB tabulky)
- podobný projekt - univerzity v Bochumi a Kielu

A5/1



Obrázek: Upozornění na nešifrovanou komunikaci

3G sítě

- přechod ze 2G sítí není jasně odlišitelný
- spíše soubor norem než nová technologie
- používá blokové šifrování KASUMI (A5/3)
- první článek o možnostech prolomení - 2001 (Kühn)
- 2005 (Biham, Dunkelman, Keller) - prolomení se znalostí 2^{54} bitů plaintextu, náročnost $2^{76,1}$

3G sítě

- přechod ze 2G sítí není jasně odlišitelný
- spíše soubor norem než nová technologie
- používá blokové šifrování KASUMI (A5/3)
- první článek o možnostech prolomení - 2001 (Kühn)
- 2005 (Biham, Dunkelman, Keller) - prolomení se znalostí 2^{54} bitů plaintextu, náročnost $2^{76,1}$

3G sítě

- přechod ze 2G sítí není jasně odlišitelný
- spíše soubor norem než nová technologie
- používá blokové šifrování KASUMI (A5/3)
- první článek o možnostech prolomení - 2001 (Kühn)
- 2005 (Biham, Dunkelman, Keller) - prolomení se znalostí 2^{54} bitů plaintextu, náročnost $2^{76,1}$

3G sítě

- přechod ze 2G sítí není jasně odlišitelný
- spíše soubor norem než nová technologie
- používá blokové šifrování KASUMI (A5/3)
- první článek o možnostech prolomení - 2001 (Kühn)
- 2005 (Biham, Dunkelman, Keller) - prolomení se znalostí 2^{54} bitů plaintextu, náročnost $2^{76,1}$

3G sítě

- přechod ze 2G sítí není jasně odlišitelný
- spíše soubor norem než nová technologie
- používá blokové šifrování KASUMI (A5/3)
- první článek o možnostech prolomení - 2001 (Kühn)
- 2005 (Biham, Dunkelman, Keller) - prolomení se znalostí 2^{54} bitů plaintextu, náročnost $2^{76,1}$

bezpečnost MT dnes

- kdyby někdo chtěl plošně odposlouchávat MT, nebude využívat předchozí útoky
- s nástupem Smart Phones se otevřeli netušené možnosti, které ale nesouvisí s kryptoanalýzou
- uživatelé sami mohou instalovat aplikace, které mají v telefonu relativně volnou ruku
- malaware, trojan - jako na PC
- vlády samy vyvíjejí vlastní software pro vysoce postavené politky
- mediálně známé případy: B. Obama, A. Merkel

bezpečnost MT dnes

- kdyby někdo chtěl plošně odposlouchávat MT, nebude využívat předchozí útoky
- s nástupem Smart Phones se otevřeli netušené možnosti, které ale nesouvisí s kryptoanalýzou
- uživatelé sami mohou instalovat aplikace, které mají v telefonu relativně volnou ruku
- malaware, trojan - jako na PC
- vlády samy vyvíjejí vlastní software pro vysoce postavené politky
- mediálně známé případy: B. Obama, A. Merkel

bezpečnost MT dnes

- kdyby někdo chtěl plošně odposlouchávat MT, nebude využívat předchozí útoky
- s nástupem Smart Phones se otevřeli netušené možnosti, které ale nesouvisí s kryptoanalýzou
- uživatelé sami mohou instalovat aplikace, které mají v telefonu relativně volnou ruku
- malaware, trojan - jako na PC
- vlády samy vyvíjejí vlastní software pro vysoce postavené politky
- mediálně známé případy: B. Obama, A. Merkel

bezpečnost MT dnes

- kdyby někdo chtěl plošně odposlouchávat MT, nebude využívat předchozí útoky
- s nástupem Smart Phones se otevřeli netušené možnosti, které ale nesouvisí s kryptoanalýzou
- uživatelé sami mohou instalovat aplikace, které mají v telefonu relativně volnou ruku
- malaware, trojan - jako na PC
- vlády samy vyvíjejí vlastní software pro vysoce postavené politky
- mediálně známé případy: B. Obama, A. Merkel

bezpečnost MT dnes

- kdyby někdo chtěl plošně odposlouchávat MT, nebude využívat předchozí útoky
- s nástupem Smart Phones se otevřeli netušené možnosti, které ale nesouvisí s kryptoanalýzou
- uživatelé sami mohou instalovat aplikace, které mají v telefonu relativně volnou ruku
- malaware, trojan - jako na PC
- vlády samy vyvíjejí vlastní software pro vysoce postavené politky
- mediálně známé případy: B. Obama, A. Merkel

bezpečnost MT dnes

- kdyby někdo chtěl plošně odposlouchávat MT, nebude využívat předchozí útoky
- s nástupem Smart Phones se otevřeli netušené možnosti, které ale nesouvisí s kryptoanalýzou
- uživatelé sami mohou instalovat aplikace, které mají v telefonu relativně volnou ruku
- malaware, trojan - jako na PC
- vlády samy vyvíjejí vlastní software pro vysoce postavené politky
- mediálně známé případy: B. Obama, A. Merkel

Konec

Děkuji za pozornost