Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Kryptológia - úvod

M. Stanek

KPMG
cutting through complexity™

Kryptológia - úvod

Martin Stanek

Témy

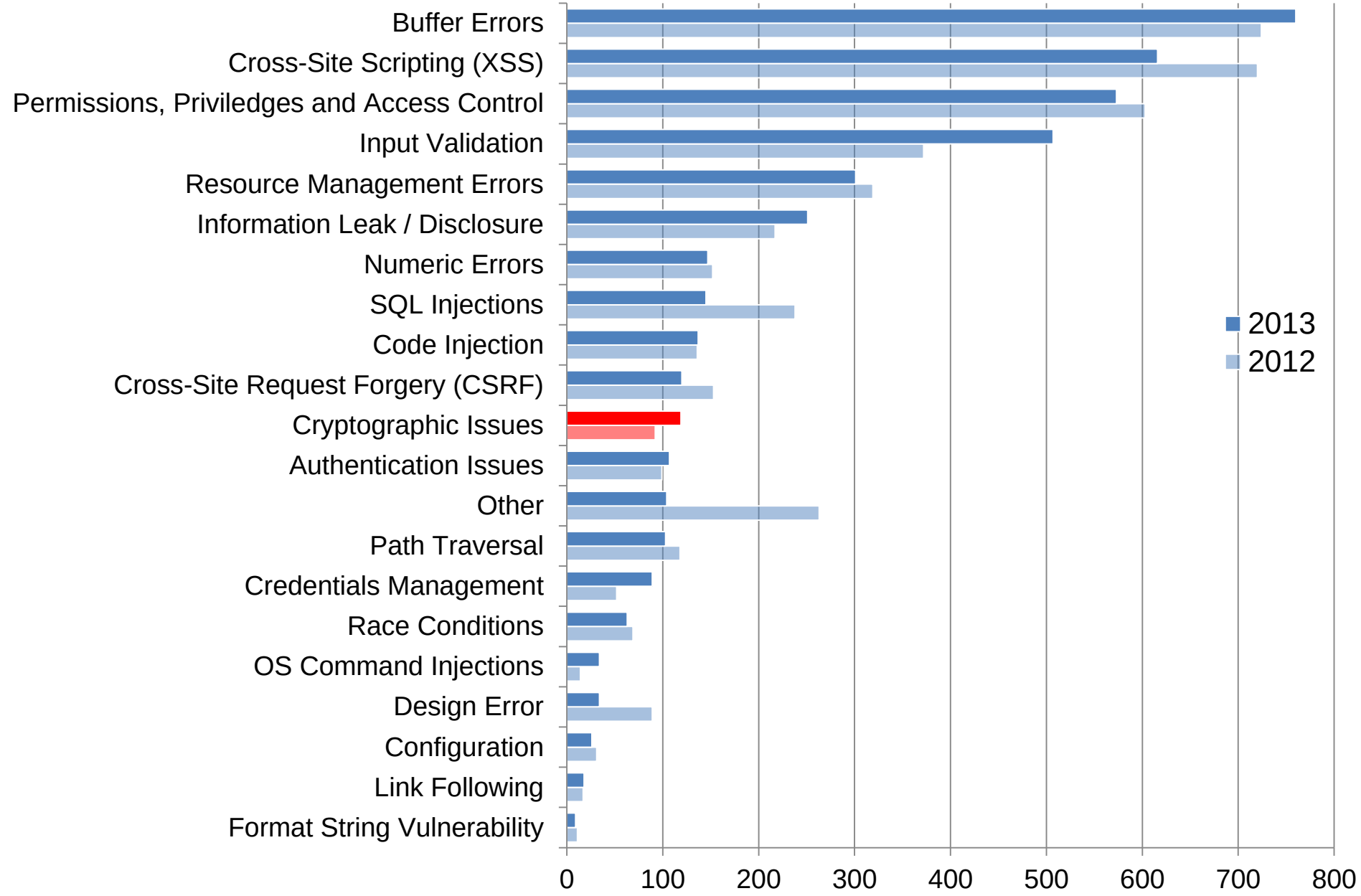
1. Úvod (základné pojmy)
2. Symetrické šifry
3. Asymetrické šifry
4. Hašovacie funkcie a autentizačné kódy
5. Digitálne podpisy
6. Protokoly pre autentizáciu a dohodnutie kľúča
7. Implementácia

Vybrané témy zamerané na kryptoanalýzu

Kryptografia ako súčasť IB

- Kryptografia a kryptoanalýza
- Požiadavky: dôvernosť, integrita, autentickosť, nepopretie autorstva/doručenia a pod.
- Kryptografia nie je odpoveďou na všetky bezpečnostné požiadavky
  - Dostupnosť (redundancia), bezpečný softvér a pod.
- Kryptografia nie je celou odpoveďou
  - Nepoužiteľná alebo zraniteľná bez ďalších opatrení: správa kľúčov, riadenie prístupu a pod.

Počty zraniteľností publikovaných v rokoch 2012 a 2013 podľa NVD



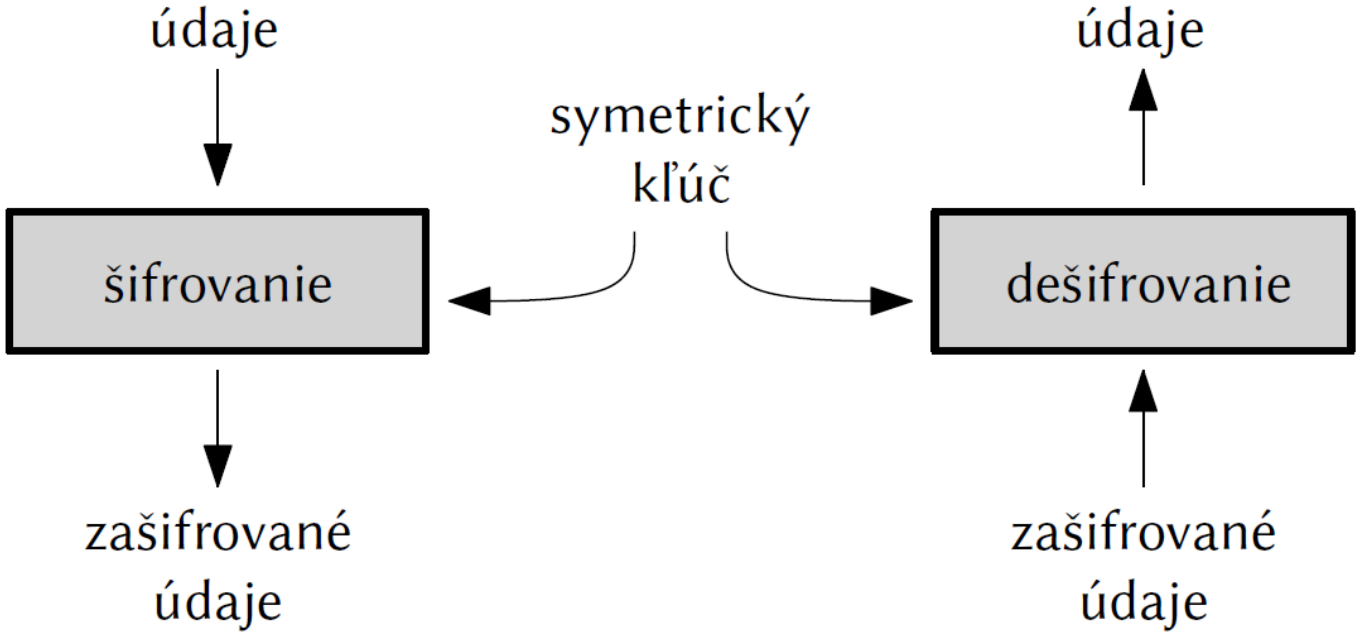
Kryptografické konštrukcie

- Obvykle používané:
  - Šifrovanie, digitálne podpisy, autentizačné kódy, protokoly pre autentizáciu a distribúciu kľúča
- Menej obvyklé:
  - Zdieľanie tajomstva, onion routing, volebné protokoly, elektronické peniaze a pod.
- „Exotické“:
  - Súkromné získavanie informácií, plne homomorfné šifrovanie a pod.

- Očakávame: efektívnosť, korektnosť a bezpečnosť

Základné pojmy

- Dôvernosť dát – šifrovanie
- Symetrická šifra
  - Schéma: generovanie kľúča, šifrovanie, dešifrovanie
  - otvorený text, šifrový/zašifrovaný text, kľúč



Posuvná šifra

- Otvorený text – reťazec znakov nad nejakou abecedou

  napr. A: 0, B: 1, C: 2, ..., Z: 25
- Kľúč *k* – určuje cyklický posun abecedy o *k* pozícií
- Šifrovanie – každý znak posunutý o *k* pozícií
- Dešifrovanie – posun opačným smerom
- Príklad:

  k = 25: IBM $\rightarrow$ HAL

  k = 1: DNES $\rightarrow$ EOFT

- Triviálny útok: vyskúšať všetky kľúče
  (útok úplným preberaním)

Jednoduchá substitučná šifra

- Podstatne viac kľúčov ako pre posunú šifru
- Kľúč – permutácia znakov abecedy, napr.:

  ABCDEFGHIJKLMNOPQRSTUVWXYZ

  PLQAOKWSIJEDUHRFTGZYMXNCBV
- Šifrovanie – každý znak nahradený podľa kľúča
- Dešifrovanie – použitie inverznej permutácie
- Príklad:

  ZAJTRA $\rightarrow$ VPJYGP
- Veľký priestor kľúčov: N! = 25! $\approx 2^{83,7}$
- Útok: frekvenčná analýza znakov, porovnávanie vzoriek

Príliš historické?

- CVE-2011-3685 – ochrana uložených používatelských mien a hesiel (Tembria Server Monitor),
- CVE-2000-0326 – ochrana posielaných hesiel medzi klientom a serverom (Meeting Maker)
- Čílski priekupníci drog (2010)

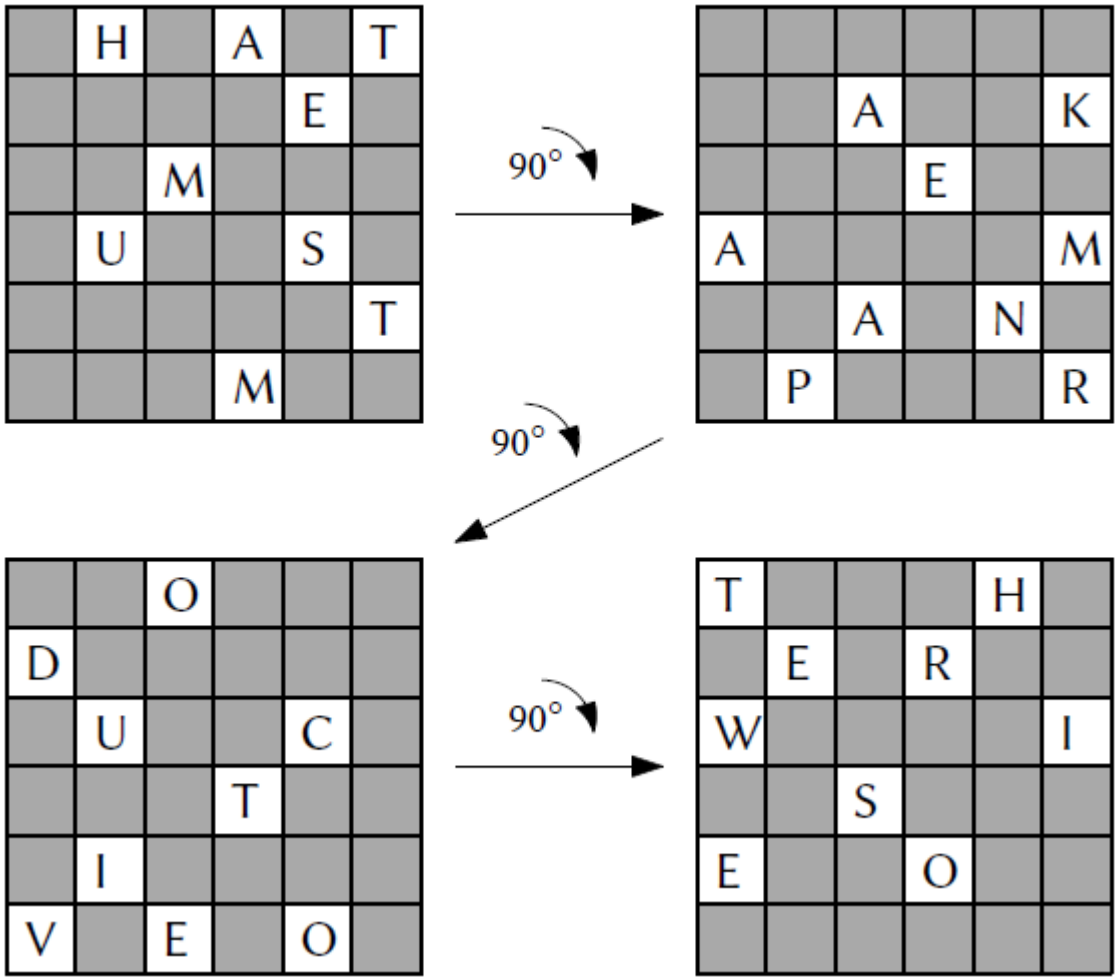
Fleissnerova mriežka

- Permutačná (transpozičná) šifra – znaky sa nemenia, mení sa len ich poradie
- Fleissnerova mriežka
  - Otáčanie štvorcovej mriežky (napr.) $2n$ x $2n$ okolo stredu
  - Štvrtina políčok „vyrezaná“ (pri otočení sa odkryjú vždy iné)
  - Krátkodobé používanie nemeckou armádou v 1. sv. vojne
- Kľúč – otvorené pozície v mriežke
  - Počet kľúčov: 4^{n*n}

    n = 3 (teda mriežka 6 x 6): $4^9 \approx 2^{18}$

    n = 6 (teda mriežka 12 x 12): $4^{36} \approx 2^{72}$

Fleissnerova mriežka – príklad



Hate must make a man productive.
Otherwise one might as well love.

Karl Kraus

T	H	O	A	H	T
D	E	A	R	E	K
W	U	M	E	C	I
A	U	S	T	S	M
E	I	A	O	N	T
V	P	E	M	O	R

Útoky na šifry – ciele?

- Zistiť použitý kľúč?
- Dešifrovať konkrétny šifrový text?
- Zistiť čiastočnú informáciu o otvorenom texte (napr. rozlíšiť, či je OT „áno“, „nie“ alebo niečo iné)?

- Prakticky: odolnosť voči „všetkým známym útokom“
- Formálnejšie prístupy: real-or-random, find-then-guess, left-or-right, ...

- Z hľadiska šifry (a teda zabezpečenia dôvernosti) neriešime útoky typu „zmysluplná manipulácia ŠT“, ...
  - Iné kryptografické konštrukcie

Útoky na šifry – predpoklady

- Možnosti a rastúca sila útočníka
- COA (Ciphertext Only Attack) – len so znalosťou ŠT
- KPA (Known Plaintext Attack) – so znalosťou OT
- CPA (Chosen Plaintext Attack) – s možnosťou voľby OT
- CCA (Chosen Ciphertext Attack) – s možnosťou voľby ŠT
- Ilustrácia sily útokov pre jednoduchú substitučnú šifru
  - COA – frekvenčná analýza
  - KPA – poznáme časť kľúča (pre všetky znaky v známom OT)
  - CPA – zvolíme OT celú abecedu ABCD...Z a ŠT je kľúč
  - CCA – podobne ako CPA, jednoduchšie to už nebude
- Asymetrické šifry – minimum je CPA (každý vie šifrovať)

Šifry a iné kryptografické konštrukcie je potrebné navrhovať a používať tak, že počítame s najsilnejším útočníkom s najmenšími cieľmi.

Ak je konštrukcia bezpečná v takomto prípade, tak bude bezpečná aj pred slabším útočníkom alebo pred útočníkom s „ambicióznejším“ cieľom.

Absolútne bezpečná šifra

- Idea: znalosť šifrového textu nepomôže útočníkovi v získaní akejkoľvek informácie o otvorenom texte (okrem jeho dĺžky).

- COA scenár
- Apriórna pravdepodobnosť OT je rovnaká ako aposteriórna pravdepodobnosť OT pri znalosti ŠT.

One-time pad

- Príklad absolútne bezpečnej šifry
- Abeceda: {0,1}, Otvorený text: $p \in \{0,1\}^n$, Kľúč: $k \in \{0,1\}^n$
- Šifrovanie: $c = p \oplus k$ (XOR po bitoch)
- Dešifrovanie: $c \oplus k = (p \oplus k) \oplus k = p \oplus (k \oplus k) = p$
- Príklad:

```
OT:    1011000
kľúč:  0111011
ŠT:    1100011
```

- Praktický problém: dĺžka kľúča rovnaká ako dĺžka OT, ŠT
- Dôverná a dôveryhodná distribúcia kľúča

One-time pad (2)

- Prečo absolútna bezpečnosť?
- Intuitívne: nech c je ŠT, môže byť OT nejaké p^*?

  áno, ak $k^* = c \oplus p^*$

Predpoklady pre bezpečnosť:

1. Nezávislé a rovnako pravdepodobné kľúče.
2. Nový kľúč generovaný pre každý otvorený text.

Čo ak neplatia predpoklady?

1. ... – aposteriórne pravdepodobnosti budú iné
2. ... – two-time pad problém

Two-time pad problém

- Viacnásobné použitie kľúča (one-time pad, prúdová šifra):

$$c1 = p1 \oplus k$$

$$c2 = p2 \oplus k$$

- Sčítaním ŠT c1 a c2 dostaneme:

$$c1 \oplus c2 = (p1 \oplus k) \oplus (p2 \oplus k) = p1 \oplus p2$$

- Bez vplyvu kľúča, možné lúštiť (automatizovane)
- Idea:
  - Model jazyka (pravdepodobnosti znakov pri známom prefixe)
  - Každý bajt $p1 \oplus p2$ má 256 možností vzniku
  - Hľadanie najpravdepodobnejšej „cesty“ medzi možnosťami

Moderné symetrické šifry

- Blokové a prúdové šifry
- Blokové šifry
  - Definované pre pevnú dĺžku vstupu (blok)
  - Realizujú permutáciu na veľkej „abecede“
- Prúdové šifry
  - Generátor pseudo-náhodných znakov
  - Ako one-time pad, len kľúč je vytváraný ako bežiaci kľúč z krátkeho kľúča (teda bez bezpečnosti one-time pad šifry)
  - Obvykle binárne aditívne
- Optimalizované na používaný hardvér, platformu

Kerckhoffsov princíp

- Bezpečnosť kryptografického systému nesmie závisieť na utajení spôsobu fungovania (algoritmu) ale výlučne na utajení kľúčov (symetrických alebo súkromných).

Protivník pozná systém.

- Neznamená to, že všetky detaily treba zverejniť.
- Kľúče nemajú byť „konštantami“.
- Nevyhnutnosť pre interoperabilitu a štandardizáciu

Kerckhoffsov princíp – príklady

- RC4 (1987) – anonymne zaslaný na mailing list (1994)
- A5/1 (1987) – algoritmus získaný reverzným inžinierstvom (1999)
- CSS (1996) – reverzné inžinierstvo ... DeCSS (1999)
- Megamos Crypto (imobilizér pre *Porsche, Audi, Bentley and Lamborghini a pod.)* – slabiny identifikované 2013, súd vo Veľkej Británii zakázal publikovať detaily (Volkswagen)

Moderná kryptológia

1. Formálne definície bezpečnosti
   - Čo znamená bezpečná šifra, digitálny podpis, autentizačný kód, protokol?
2. Precízne formulácie predpokladov bezpečnosti
   - Predpoklady kryptografickej konštrukcie (problém, náhodnosť parametrov a pod.), možnosti útočníka.
3. Dôkazy bezpečnosti
   - Matematika

Na zamyslenie (1)

Vieme „zosilniť“ šifru viacnásobnou aplikáciou?

- Zreťazme dve alebo viaceré aplikácie šifry, použijúc nezávislé kľúče. Uvažujme jednoduchú substitučnú šifru, Fleissnerovu mriežku a one-time pad. Bude výsledná šifra bezpečnejšia ako pôvodná?

Na zamyslenie (2)

Výmena správy *m* medzi dvoma účastníkmi A a B.

1. A zašifruje *m* použitím one-time pad šifry a pošle *c*1 B.
2. B zašifruje *c*1 použitím one-time pad šifry a pošle *c*2 A.
3. A dešifruje c2 a pošle výsledok B.
4. B dešifruje a získa *m*.

- Je tento postup korektný (získa B naozaj *m*)?
- Je tento protokol bezpečný?

Na zamyslenie (3)

- Aká by bola bezpečnosť variantu posuvnej šifry, v ktorom by sme dlhšie správy šifrovali tak, že každé znak správy šifrujeme náhodne zvoleným posunom (samozrejme, v takom prípade by bol kľúč rovnako dlhý ako správa)?

Ďakujem za pozornosť