Základy kryptológie

Ing. Radovan Semančík

6. Linux weekend, Marec 2002, Bratislava

Agenda

- Úvod a história
- Šifrovacie metódy
- Autentifikačné metódy
- Prax
- Záver

Krypto-čo?

- Kryptológia: “kryptós” = zatajený, skrytý
  - Kryptografia - teória šifrovania
  - Kryptoanalýza - útoky na šifry
- 7 st.p.n.l., Sparta, “skytalé”
- 1 st.p.n.l., Július Cézar
- 15 st. n.l. Arábia, Benátky, Rím
- 17 st. n.l. rozmach kryptografie

ENIGMA

BGS
Business Global Systems

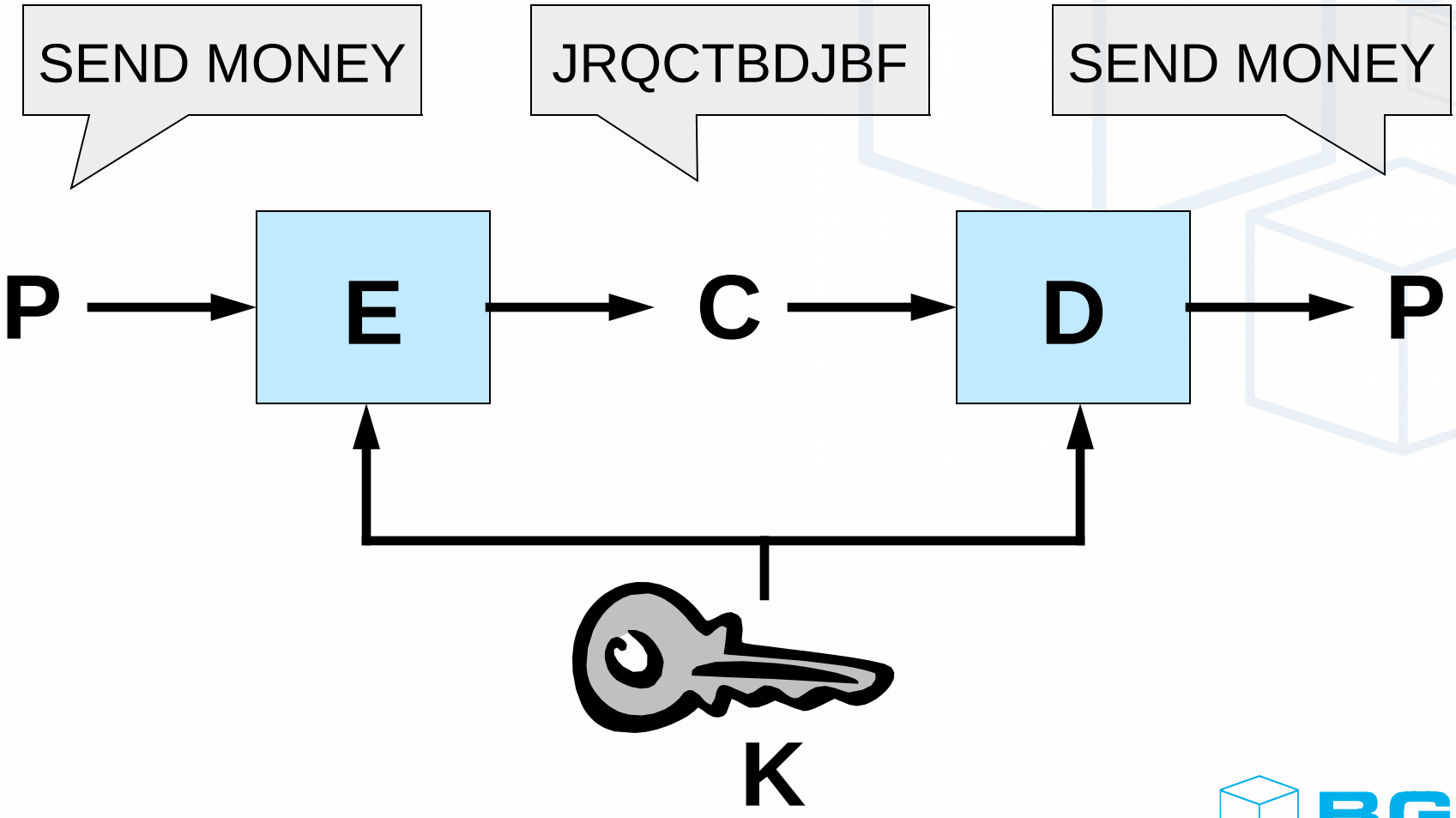
20. storočie

- 2. svetová vojna: ENIGMA
- Studená vojna
- DES: IBM 1970s, štandard od 1976
- **1976: W. Diffie, M.E. Hellman**
  - “New directions in cryptography”
  - Začiatok asymetrickej kryptografie
- Oct 2000: AES (Rijndael)

Agenda

- Úvod a história
- Šifrovanie metódy
- Autentifikačné metódy
- Prax
- Záver

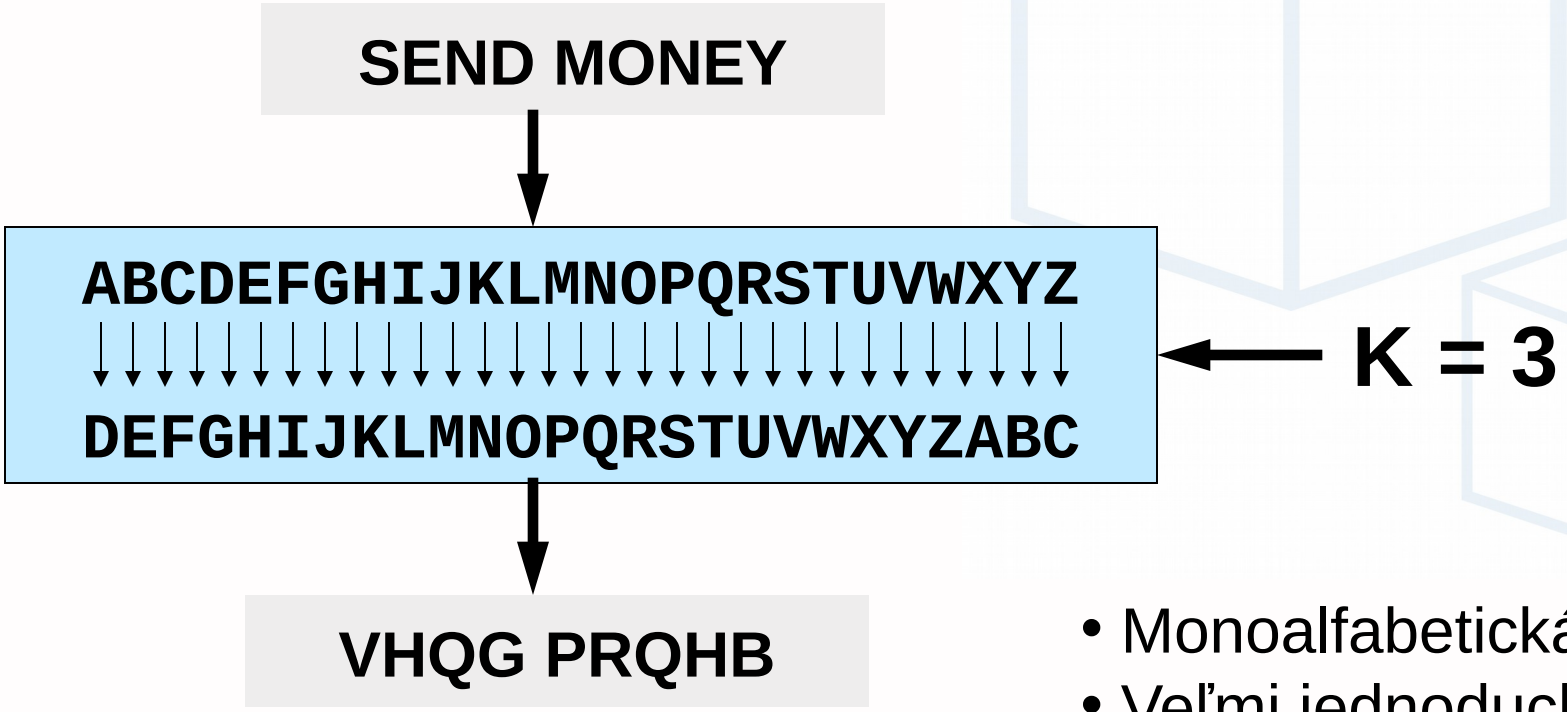
Kryptosystém



Šifrovanie
vs
kódovanie

BGS
Business Global Systems

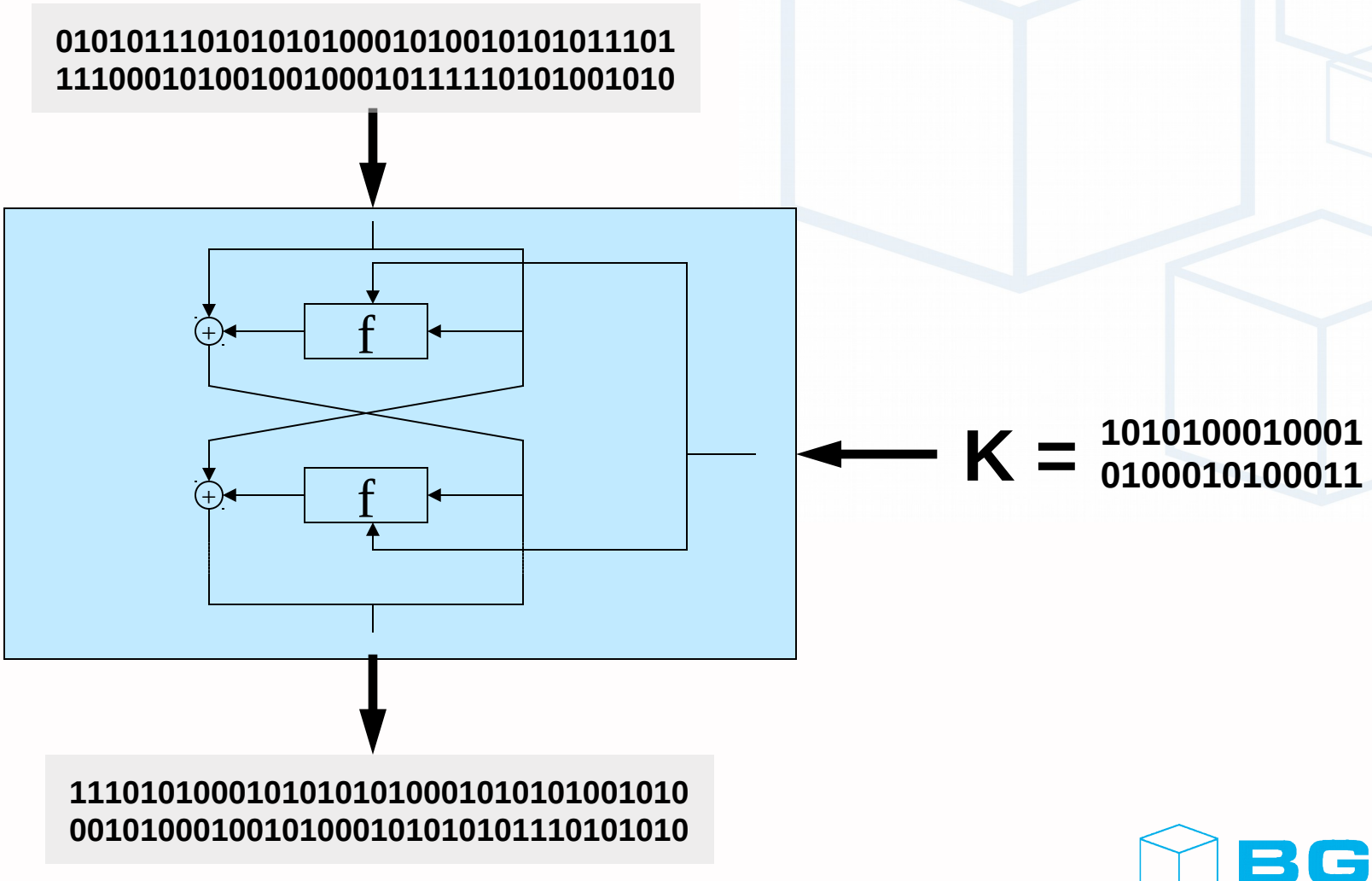
Cézarova šifra



- Monoalfabetická šifra
- Veľmi jednoduchá

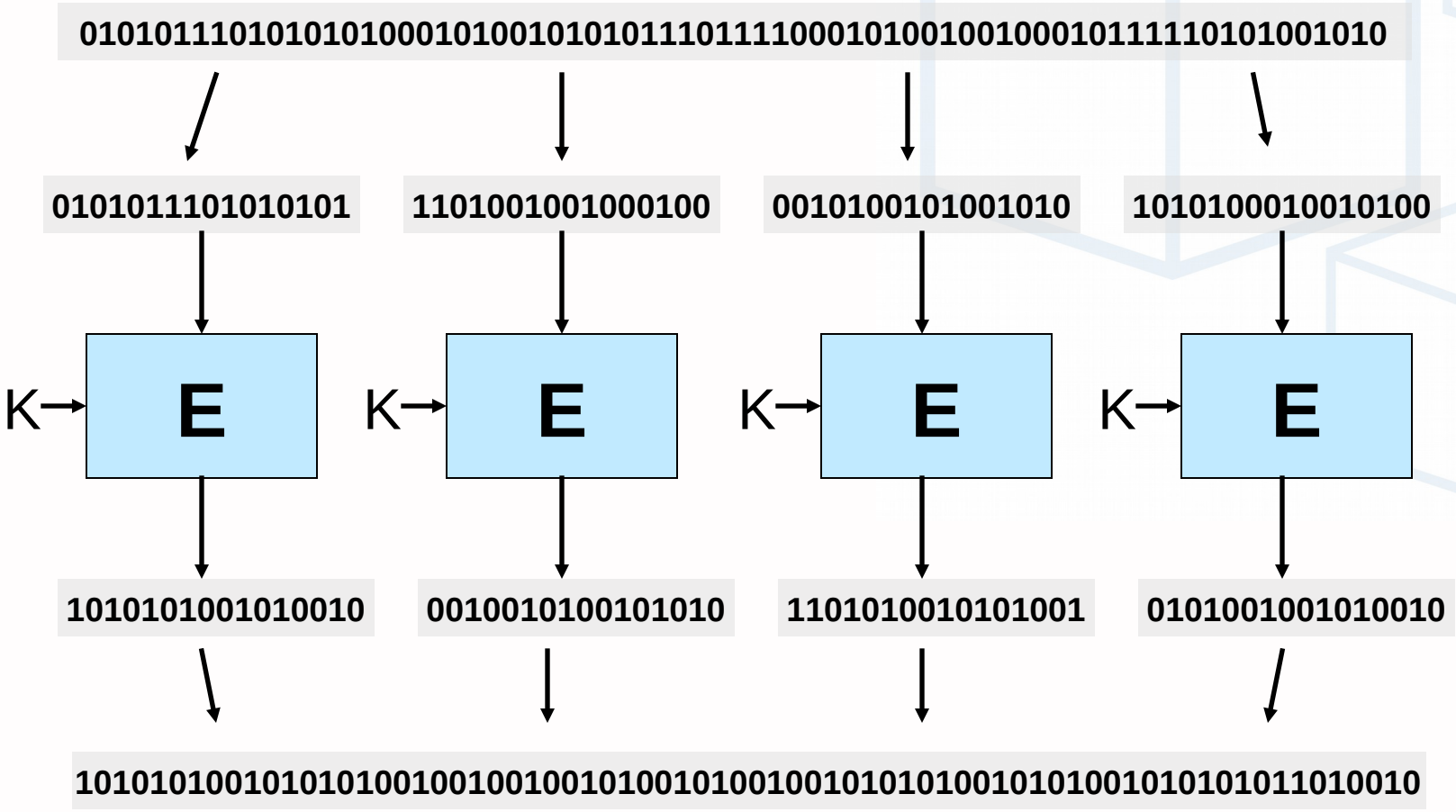
BGS
Business Global Systems

Moderné šifry



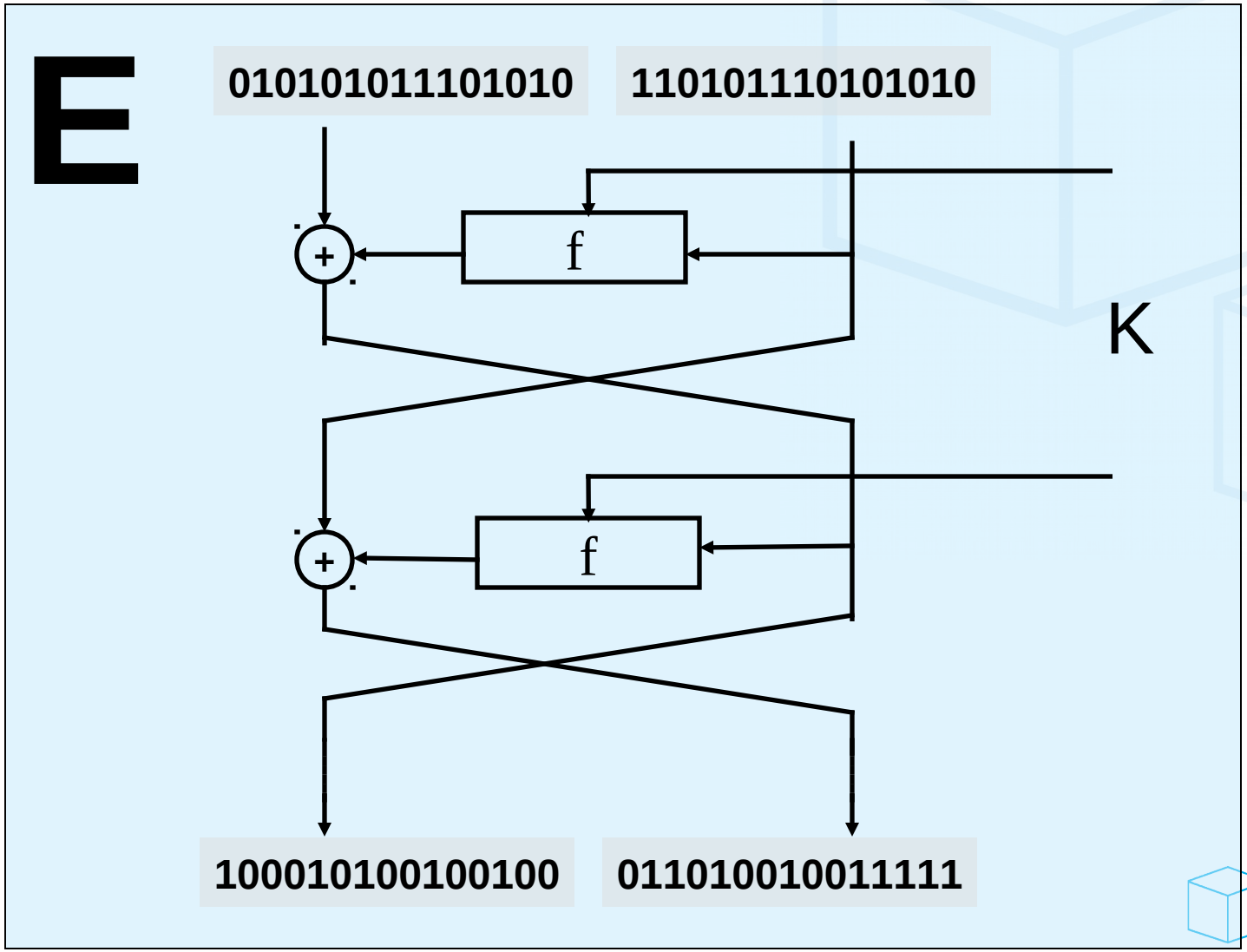
BGS
Business Global Systems

Bloková šifra



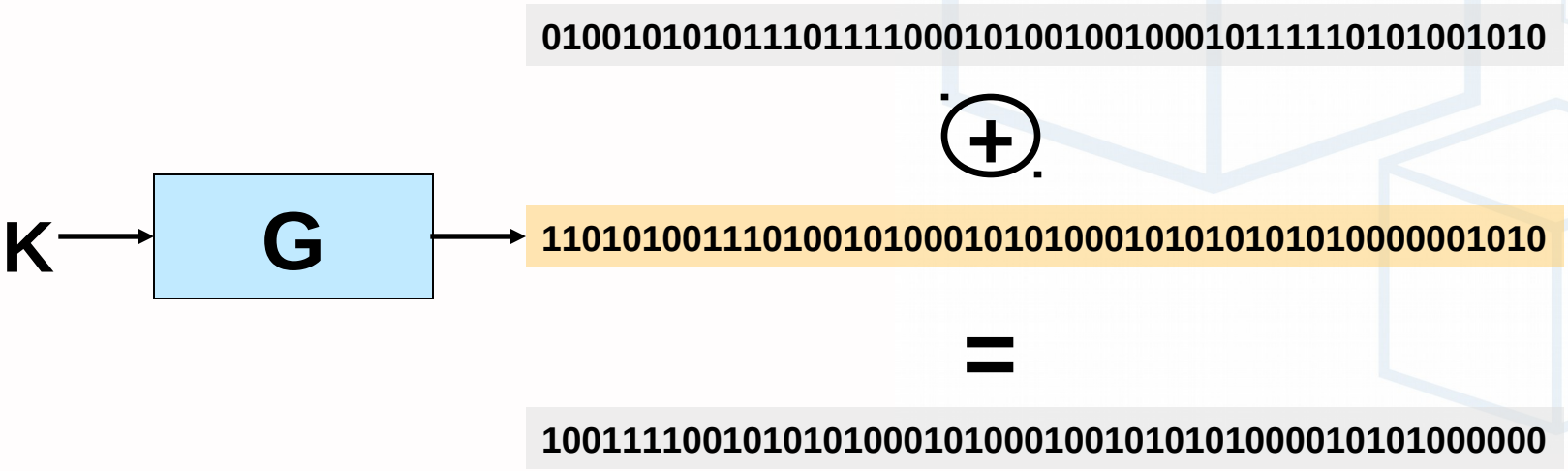
BGS
Business Global Systems

Feistelovská bloková šifra



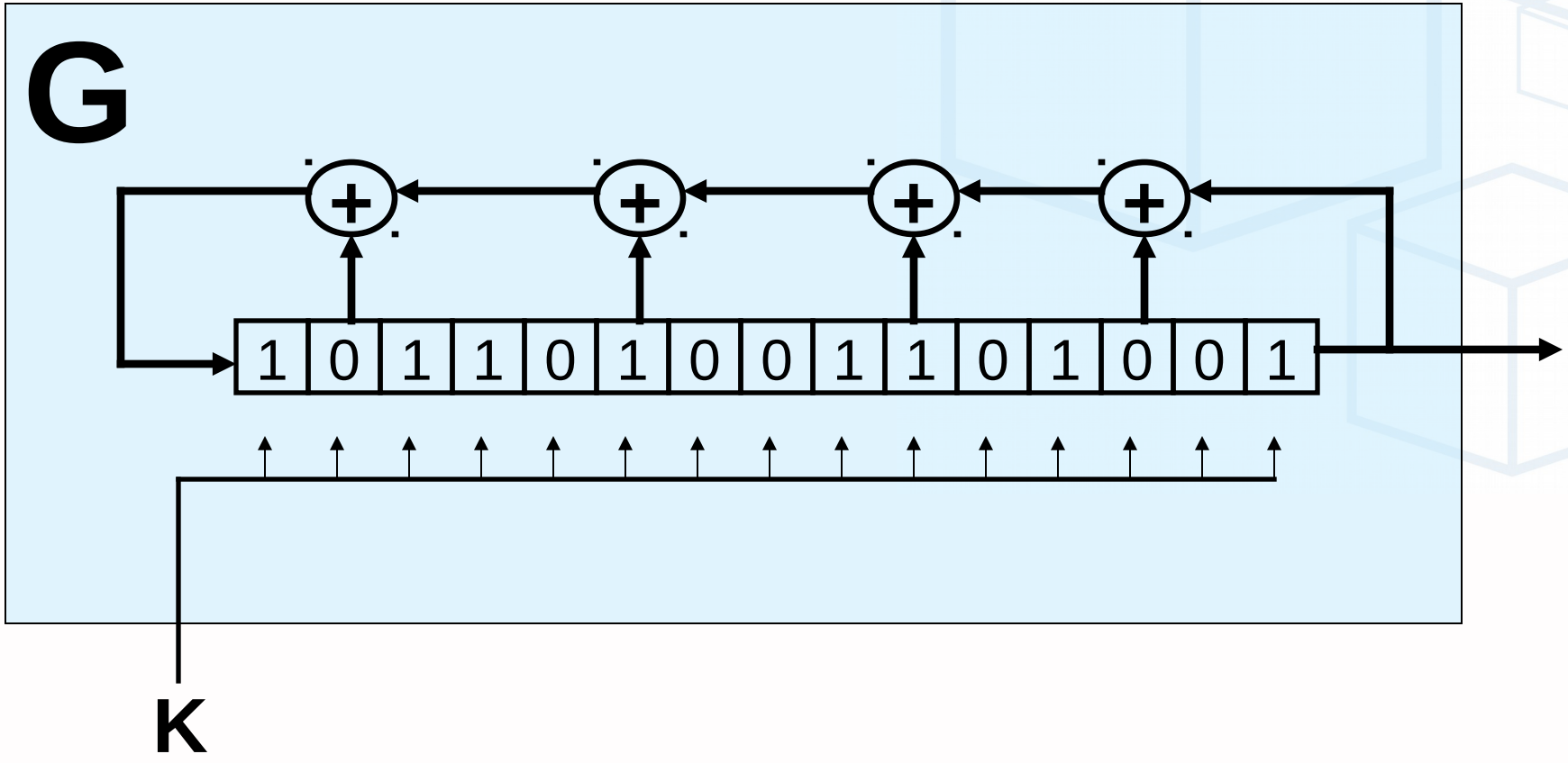
BGS
Business Global Systems

Prúdová šifra



BGS
Business Global Systems

Linear **F**eedback **S**hift **R**egister

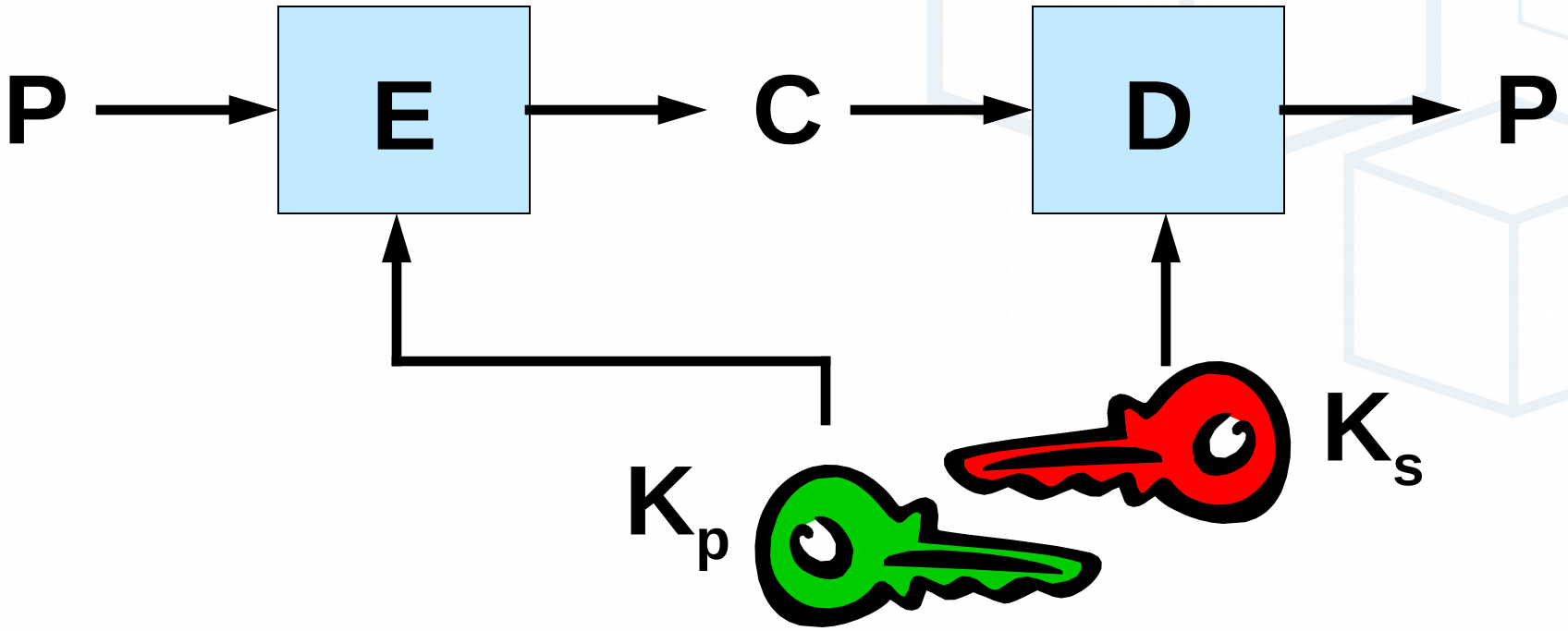


BGS
Business Global Systems

Prúdové vs Blokové šifry

- Blokové šifry
  - Dobre preskúmané, veľa implementácii
  - Módy činnosti (ECB,CBC,CFB, …)
  - DES, IDEA, Blowfish, Twofish, Rijndael(AES)
- Prúdové šifry
  - Málo preskúmané
  - Rýchle, najmä na HW
  - RC4, A5, LEVIATHAN, SEAL

Asymetrická kryptografia



Kľúčový pár

Jednoduchý kľúčový manažment

BGS
Business Global Systems

Ťažké problémy

- Faktorizácia (RSA)
  - n = p.q … p,q - prvočísla
  - ľahké: máme p,q a chceme nájsť n
  - ťažké: máme n, chceme nájsť p,q
- Diskrétne logaritmy (DH, ElGamal)
  - $y = g^x \bmod t$
  - ľahké: máme g,t,x a chceme nájsť y
  - ťažké: máme g,t,y a chceme nájsť x

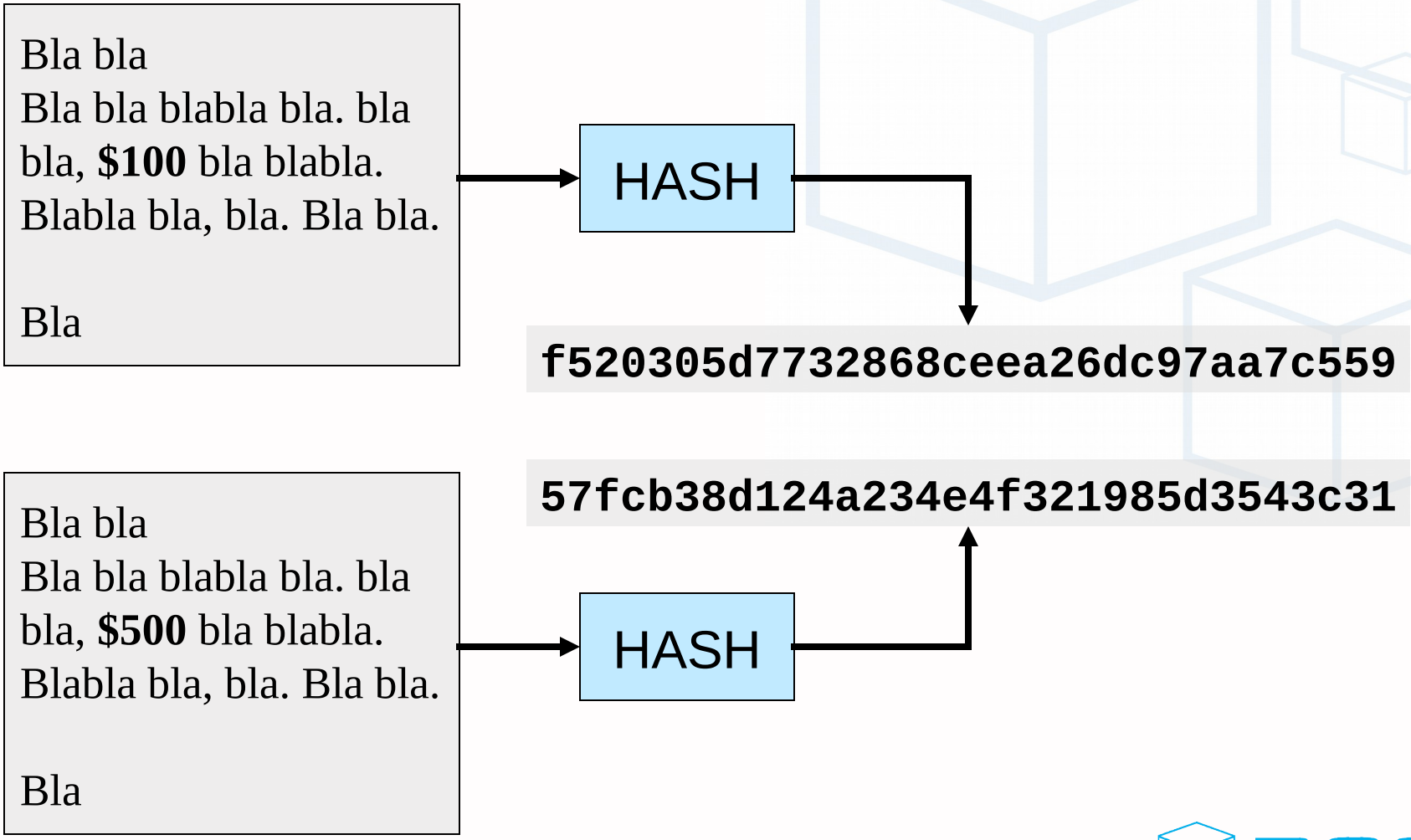
Kľúče, kľúče, kľúče

- Symetrická kryptografia
  - bezpečný kanál na distribúciu kľúčov
  - n(n-1)/2 zdieľaných kľúčov
  - kľúče 56-256 bitov
- Asymetrická kryptografia
  - Autentifikácie kľúčov - certifikáty
  - n kľúčových párov
  - kľúče 512-2048 bitov

Agenda

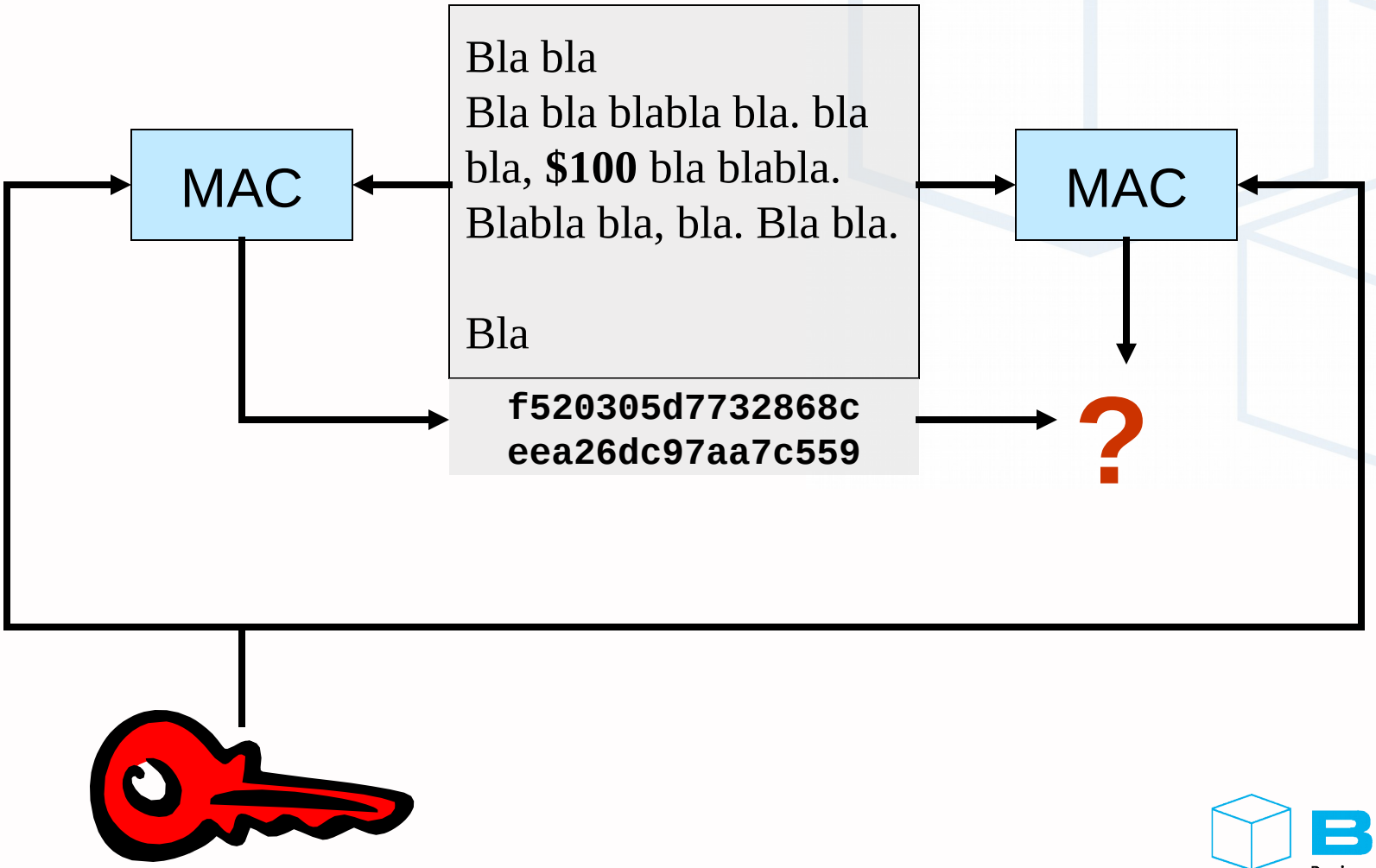
- Úvod a história
- Šifrovanie metódy
- Autentifikačné metódy
- Prax
- Záver

Hash



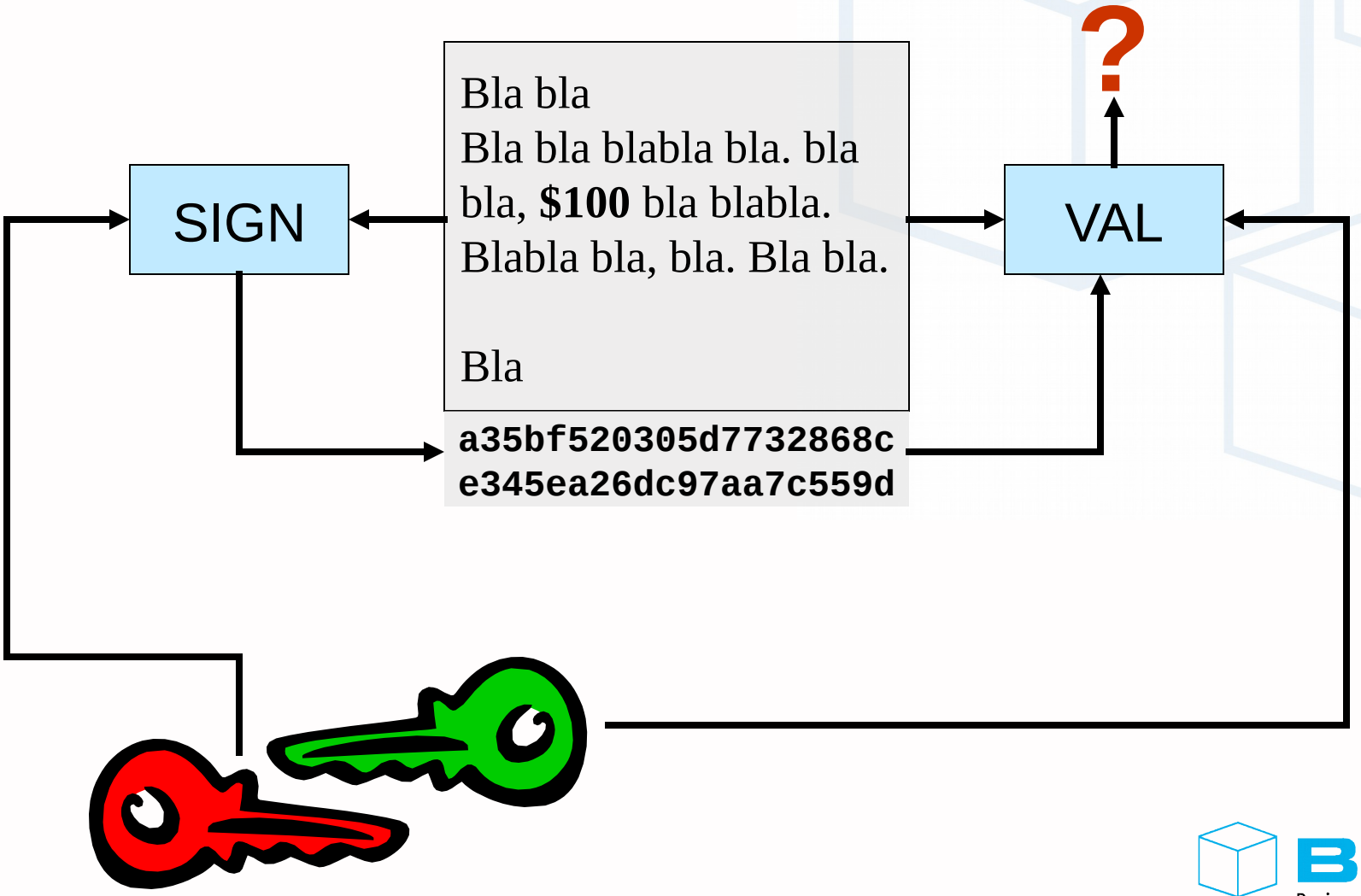
BGS
Business Global Systems

Message **A**uthentication **C**ode



Business Global Systems

Digitálny podpis



Business Global Systems

Poznámky

- HASH
  - bez kľúča, potrebuje bezpečný kanál
- MAC
  - symetrické = rýchle
- Digitálny podpis
  - asymetrické = pomalé
  - podpisuje sa väčšinou len HASH
  - kto podpísal? Komu patrí kľúč? - certifikáty

Dĺžka kľúča

Dĺžka kľúča

- Symetrické
  - 40 bit: Buaahaaahahahahahahahaa
  - 56 bit: dnes už nebezpečné, cca 4h
  - 168 bit 3DES: Akceptovateľné (cca $O(2^{100})$)
  - 128 bit: Bezpečné (pre bežné použitie)
  - 256 bit: nový štandard

Business Global Systems

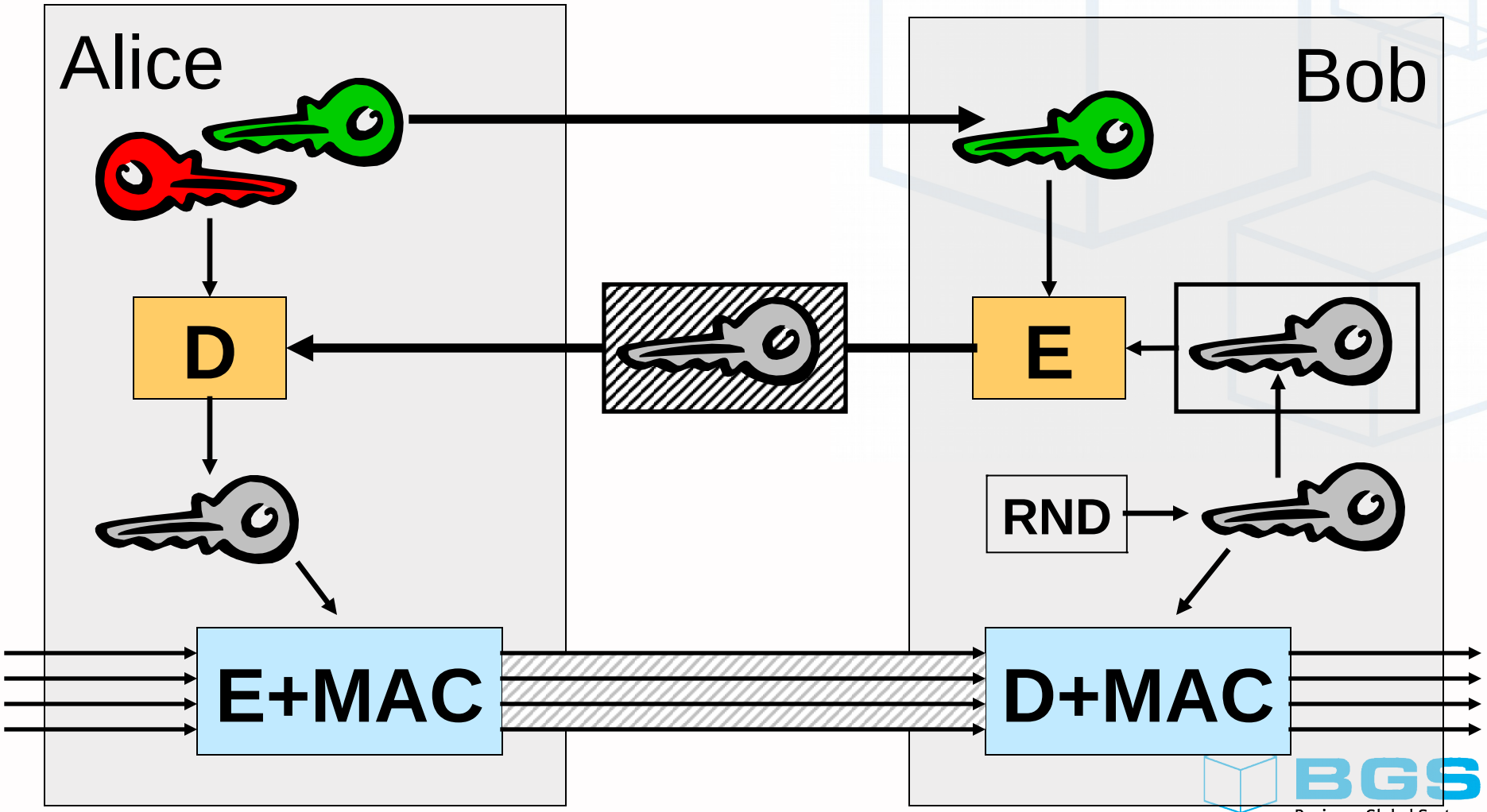
Dĺžka kľúča

- Asymetrické (RSA)
  - 256 bit: nebezpečné
  - 512 bit: rizikové
  - 1024 bit: štandard pre osobné kľúče
  - 2048 bit: štandard pre CA
  - 4096 bit: už aj také sa používajú

Agenda

- Úvod a história
- Šifrovanie metódy
- Autentifikačné metódy
- Prax
- Záver

Key exchange (RSA)



Kryptoanalýza

- Útoky
  - Ciphertext only (poznám len C)
  - Know plaintext (poznám páry P,C)
  - Choosen planintext (volím P, pozorujem C)
  - Choosen ciphertext (volím C, pozorujem P)
  - Adaptive CPA a CCA
- Úloha: nájsť kľúč

Ako je to vlastne ...

- Nepodmienečne bezpečná šifra
  - Vernamova šifra (One time pad)
    - nepraktická … aj keď …..
- Bezpečnosť ostatných nie je istá
  - Je faktorizácia nutná na zlomenie RSA?
  - Je faktorizácia NP-úplný problém?
  - Je diskrétny logaritmus NP-úplný problém?
  - atď...

Eh?

BGS
Business Global Systems

Coming soon ...

Internet security

BGS
Business Global Systems

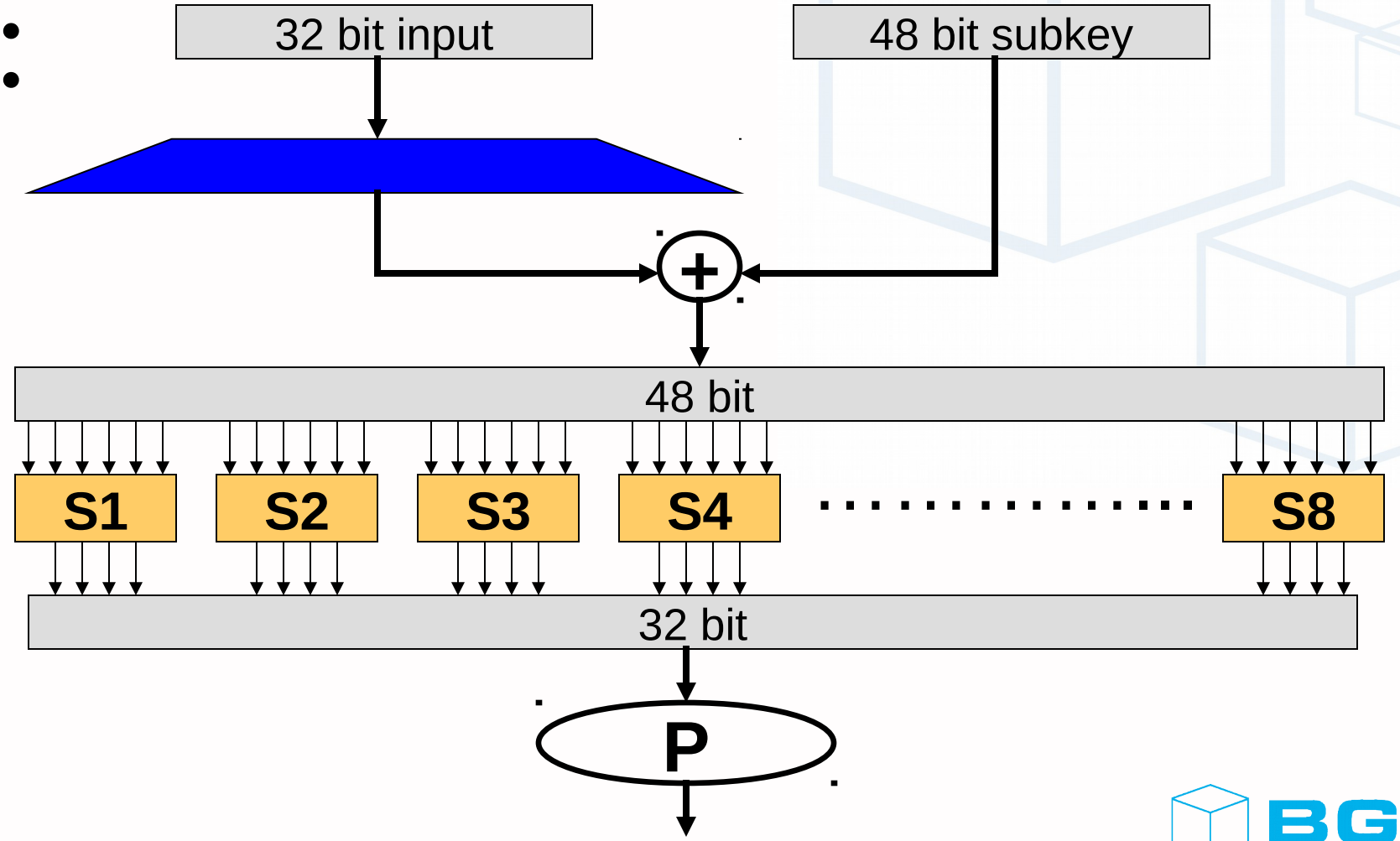
Ďakujem za pozornosť

Ing. Radovan Semančík
Business Global Systems
semancik@bgs.sk

BGS
Business Global Systems

DES round

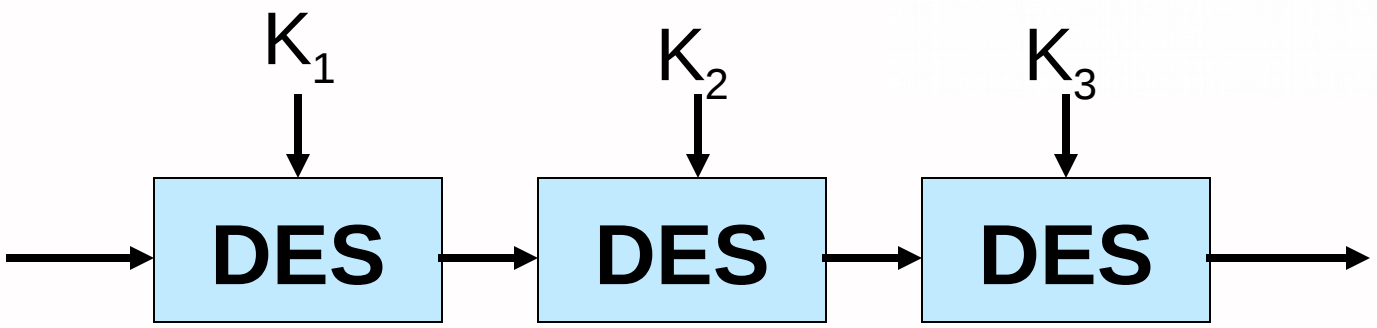
f:



BGS
Business Global Systems

TripleDES (3DES)

- Je DES grupa? …. nie je!
- Módy:
  - EEE3, EDE3, EEE2, EDE2



BGS
Business Global Systems

RSA

- N=p.q … p,q - veľké prvočísla

$\forall$ $\varphi(N) = (p-1)(q-1)$

- $1 < e < \varphi(N)$, $\gcd(e, \varphi(N))=1$
- $1 < d < \varphi(N)$, $\gcd(d, \varphi(N))=1$, $e.d \equiv 1 \bmod \varphi(N)$
- Kľúče: verejný = (e,N) súkromný = (d,N)
- E: $c \equiv m^e \bmod N$
- D: $m \equiv c^d \bmod N$

BGS
Business Global Systems