Kryptografické systémy
generovanie a distribúcia kľúčov

doc. RNDr. Jozef Jirásek, PhD.

ZS 2023

Symetrické kľúče

- veľký počet symetrických kľúčov ~ n^2
- KEK dlhodobý (longterm, master key) kľúč
- relačný (session) kľúč
- dočasný (ephemeral) kľúč - (zmena kľúča pri dlhodobejšej relácii, dohoda na kľúči)

Doporučenie NIST pre dĺžky kľúčov (2020)

	short	do 2030			
	80	112	128	192	256
Sym	3D2K	3DES	AES-128	AES-192	AES-256
MDC	SHA-1	SHA3-224	SHA3-256	SHA3-384	SHA3-512
MAC			SHA-1	SHA-224	SHA3-512
RSA	1024	2048	3072	7680	15360
DLP	160	224	256	384	512
ECC	160	224	256	384	512

ANSI generátor relačných kľúčov

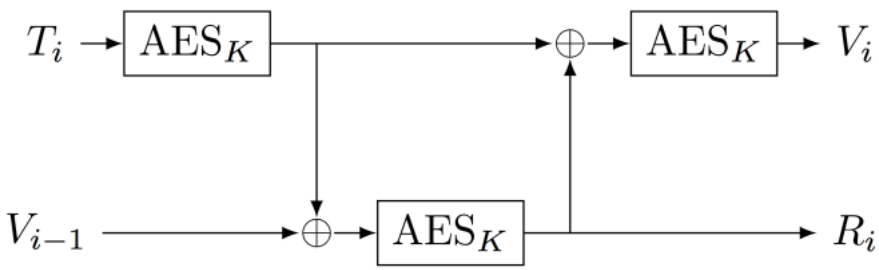
- ANSI X9.31 generátor

K dlhodobý (longterm) kľúč (Key Encoding Key)

$R_i = AES_K(V_{i-1} \oplus AES_K(T_i))$ výstup

$V_i = AES_K(R_i \oplus AES_K(T_i))$ seed (semienko)

časová pečiatka



nové semienko

semienko

výstup

dočasný (session) kľúč

po prelomení je možné získať všetky generované kľúče !

Možnosť útokov na ANSI generátor

ak niekedy získame K (napr. FortiOS firmware s pevným K),
je možné urobiť útok na generované dočasné kľúče :

ak poznáme za sebou nasledujúce dočasné kľúče R_i a R_{i+1} potom

$R_i = E(V_{i-1} \oplus E(T_i))$, $V_i = E(R_i \oplus E(T_i))$

$R_{i+1} = E(V_i \oplus E(T_{i+1}))$, $D(R_{i+1}) = V_i \oplus E(T_{i+1})$ a $V_i = D(R_{i+1}) \oplus E(T_{i+1})$

a teda $R_i \oplus E(T_i) = D(V_i) = D(D(R_{i+1}) \oplus E(T_{i+1}))$

z čoho môžeme postupnými iteráciami možných časových pečiatok
pomocou meet-in-the-middle postupu získať T_i a T_{i+1}

potom viem spočítať $V_{i+1} = E(R_{i+1} \oplus E(T_{i+1}))$ a ďalej
opäť postupnými iteráciami pečiatky T_{i+2} aj $R_{i+2} = E(V_{i+1} \oplus E(T_{i+2}))$

atď ... a potom podobne aj spätne ...

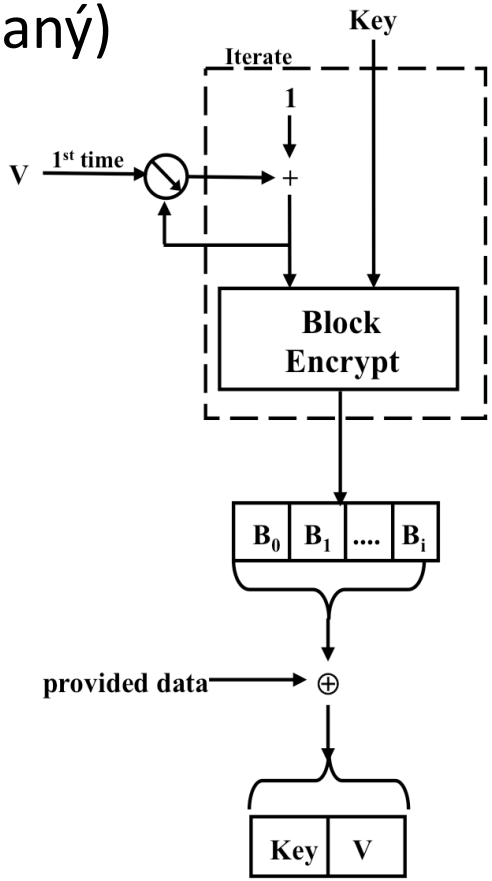
CTR_DRBG generátor

NIST SP 800-90A deterministický generátor náhodných bitov

(Dual_EC_DRBG – s EC šifrovaním – odvolaný)

HMAC_DRBG

CTR_DRBG (2015)
založený na blokovej šifre (AES)
v CTR režime + reseed



CSPRNG – kryptograficky bezpečné
generátory pseudonáhodných čísel

Kryptograficky bezpečné generátory náhodných bitov

- Blum-Blum-Shub generátor pre prvočísla p, q

$$b_0 = seed \quad b_i = b_{i-1}^2 \; mod \; pq \qquad p \equiv q \equiv 3 \; (mod \; 4)$$

$$s_i = b_i \; mod \; 2$$

predikcia nasledujúceho bitu streamu je ekvivalentná problému riešenia kvadratických rezíduí

- Blum-Micali algoritmus p – prvočíslo, g - generátor $\mathbb{Z}_p^*$

x_0 = seed $\quad x_i = g^{x_{i-1}} \; mod \; p$

$s_i = 1$ ak $x_i \leq (p-1)/2$ (inak $s_i = 0$)

predikcia je ekvivalentná DLP problému (riešenia diskrétneho logaritmu modulo p)

Dohoda na kľúči pomocou symetrickej kryptografie

ako vytvoriť bezpečný komunikačný kanál,

pokiaľ nemám možnosť priamej komunikácie

s druhou stranou ?

Dohoda na kľúči pomocou symetrickej kryptografie

Merkle‘s Puzzle (1974)

- Alica vygeneruje milión správ „toto je i-ty kľúč, kľúč je K_i “ každú zašifruje iným náhodným 50-bitovým kľúčom všetky pošle v náhodnom poradí Bobovi
- Bob náhodne vyberie jednu, hrubou silou zistí text pošle Alici len index i
- Alica a Bob môžu bezpečne používať kľúč K_i
- útočník – aj keď pozná i, musí rozbíjať hrubou silou všetky správy (~2^{70} testov)

Dohoda na kľúči so zámkami

schéma so zámkami (padlock)

pre dostatočne veľké prvočíslo p a náhodné a a b

A : zvolí kľúč K

(pre p = 2q + 1 je možné overiť, či K je generátor $\mathbb{Z}_p^*$)

A $\longrightarrow$ B : K^a mod p

B $\longrightarrow$ A : $(K^a)^b$ mod p

A $\longrightarrow$ B : $(K^{ab})^{a'}$ mod p = K^b mod p pre $a' \cdot a \equiv 1 \pmod{p-1}$

B : K = $(K^b)^{b'}$ mod p pre $b' \cdot b \equiv 1 \pmod{p-1}$

Dohoda so spoločným tajomstvom

A a B poznajú tajomstvo KAB (napr. heslo)

$A \longrightarrow B : \quad N_A$

$B \longrightarrow A : \quad N_B$

nový relačný kľúč bude $K = f(MAC_{KAB}(N_A, N_B))$

môže nasledovať autentifikácia bezpečným kanálom

GSM autentifikácia a dohoda na kľúči A3/A8

KI – autentifikačný kľúč v SIM tiež v AC (autentifikačnom centre)

BTS (base station) ⟶ A : RAND (128b)

A vypočíta $Comp128_{KI}(RAND) = SRES\ (32b)\ |\ (32b)|\ K_C\ (64b)$

A ⟶ BTS : SRES (Signed Response Number)

BTS vykomunikuje SRES s AC a overí správnosť odpovede od A

BTS dostane od AC aj K_C , ktorý použije na šifrovanú komunikáciu (pomocou prúdovej šifry A5) s A

Prenos kľúča symetrickou kryptografiou

- $A \longrightarrow B$: $E_{AB}(K)$ bez dôkazu čerstvosti
- $A \longrightarrow B$: $E_{AB}(T_A)$ s časovou pečiatkou - $K = f(K_{AB}, T_A)$
- $A \longrightarrow B$: $E_{AB}(T_A, B, K)$
- $B \longrightarrow A$: N_B s výzvou
  $A \longrightarrow B$: $E_{AB}(N_B, B, K)$
- $A \longrightarrow B$: $E_{AB}(T_A, B, F_A)$ obojstranná
  $B \longrightarrow A$: $E_{AB}(T_B, A, F_B)$ $K = f(F_A, F_B)$
- $B \longrightarrow A$: N_B obojstranná s výzvou
  $A \longrightarrow B$: $E_{AB}(N_A, N_B, B, F_A)$
  $B \longrightarrow A$: $E_{AB}(N_B, N_A, A, F_B)$ $K = f(F_A, F_B)$

Prenos kľúča dôveryhodným centrom

Dôveryhodné translačné centrum (len prenáša správy)

- Wide-Mouth Frog (WMF)

  $A \longrightarrow S$: $A, E_{AS}(T_A, B, K)$ (lepšie $E_{AS}(T_A, A, B, K)$

  $S \longrightarrow B$: $E_{BS}(T_S, A, K)$ kvôli symetrii)

- centralizovaný management (ako certifikáty)

  $A \longrightarrow S$: $A, E_{AS}(B, K)$

  $S \longrightarrow A$: $E_{BS}(K, A)$ musí byť uvedená identita A

  $A \longrightarrow B$: $E_{BS}(K, A)$ replay ? časová pečiatka

  $A \longrightarrow S$: $E_{AS}(N_A, B, K)$

  $S \longrightarrow A$: $E_{AS}(N_A, B), E_{BS}(T_S, K, A)$

  $A \longrightarrow B$: $E_{BS}(T_S, K, A)$ dá sa bez časových pečiatok ?

Generovanie kľúča v dôveryhodnom centre

Dôveryhodné distribučné centrum (generuje kľúče)

- (pull model)

  $A \longrightarrow S$: A, B

  $S \longrightarrow A$: $E_{AS}(T_S, B, K, E_{BS}(T_S, A, K))$

  $A \longrightarrow B$: $E_{BS}(T_S, A, K)$

- (push model)

  $A \longrightarrow B$: A, N_A

  $B \longrightarrow S$: A, N_A, B, N_B

  $S \longrightarrow B$: $E_{BS}(N_B, A, K), E_{AS}(N_A, B, K)$

  $B \longrightarrow A$: $E_{AS}(N_A, B, K)$

Generovanie kľúča s lístkom (tiketom)

Needham-Schroeder generovanie kľúčov v centre

- $A \longrightarrow S$: A, B, N_A
  $S \longrightarrow A$: $E_{AS}(K, B, N_A, E_{BS}(K, A))$ $E_{BS}(K, A)$ – lístok (ticket)
  $A \longrightarrow B$: $E_{BS}(K, A)$
  $B \longrightarrow A$: $E_K(N_B)$ autentifikácia
  $A \longrightarrow B$: $E_K(N_B\text{-}1)$

Systém Kerberos (AS, TGS, SS)

AS – autentifikačný server

- $A \longrightarrow AS$: A, SS, T_1 A_A = adresa A
  $AS \longrightarrow A$: $E_{pwd}(K_{ATGS}, SS, T_2, L, E_{ASTGS}(K_{ATGS}, A, A_A, SS, T_2, L))$
  TGT – ticket-granting ticket

Systém Kerberos (AS, TGS, SS)

AS – autentifikačný server

- $A \longrightarrow AS$: A, SS, T_1 A_A = adresa A
  $AS \longrightarrow A$: $E_{pwd}(K_{ATGS}, SS, T_2, L, E_{ASTGS}(K_{ATGS}, A, A_A, SS, T_2, L))$
  TGT – ticket-granting ticket

TGS – distribúcia žiadostí (lístkov) na služby (ticket-granting server)

- $A \longrightarrow TGS$: $SS, E_{ATGS}(A, A_A, T_3), E_{ASTGS}(K_{ATGS}, A, A_A, SS, T_2, L)$

  $TGS \longrightarrow A$: $E_{ATGS}(K_{ASS}, SS, T_4, E_{SSTGS}(K_{ASS}, A, A_A, SS, T_4, L'))$
  lístok na službu SS pre A na čas L'

Systém Kerberos (AS, TGS, SS)

AS – autentifikačný server

- $A \longrightarrow AS$: A, SS, T_1 A_A = adresa A
  $AS \longrightarrow A$: $E_{pwd}(K_{ATGS}, SS, T_2, L, E_{ASTGS}(K_{ATGS}, A, A_A, SS, T_2, L))$
  TGT – ticket-granting ticket

TGS – distribúcia žiadostí (lístkov) na služby (ticket-granting server)

- $A \longrightarrow TGS$: $SS, E_{ATGS}(A, A_A, T_3), E_{ASTGS}(K_{ATGS}, A, A_A, SS, T_2, L)$

  $TGS \longrightarrow A$: $E_{ATGS}(K_{ASS}, SS, T_4, E_{SSTGS}(K_{ASS}, A, A_A, SS, T_4, L'))$
  lístok na službu SS pre A na čas L'

SS – service server

- $A \longrightarrow SS$: $E_{ASS}(A, A_A, T_5), E_{SSTGS}(K_{ASS}, A, A_A, SS, T_4, L')$
  $SS \longrightarrow A$: $E_{ASS}(T_5 + 1)$

Systém Kerberos V (AS, TGS, SS)

AS – autentifikačný server

- $A \longrightarrow AS$: A, SS, L, N_1 = nonce A_A = adresa A
  $AS \longrightarrow A$: $SS, A, E_{pwd}(K_{ATGS}, L, N_1, TGS, SS), E_{ASTGS}(K_{ATGS}, A, A_A, L)$
  TGT – ticket-granting ticket

TGS – distribúcia žiadostí (lístkov) na služby (ticket-granting server)

- $A \longrightarrow TGS$: $SS, L, N_2, E_{ATGS}(A, T_1), E_{ASTGS}(K_{ATGS}, A, A_A, L)$

  $TGS \longrightarrow A$: $A, E_{ATGS}(K_{ASS}, L, N_2, SS), E_{SSTGS}(K_{ASS}, A, A_A, L)$
  lístok na službu SS pre A

SS – service server

- $A \longrightarrow SS$: $E_{ASS}(A, T_2, SN), E_{SSTGS}(K_{ASS}, A, A_A, L)$
  $SS \longrightarrow A$: $E_{ASS}(T_2, SN)$ L – interval platnosti
  SN – sekvenčné číslo žiadosti

Dohoda na kľúči Diffie-Hellmanovou výmenou

Diffie-Hellman (1976)

veľké verejne známe prvočíslo p a generátor g grupy $\mathbb{Z}_p^*$

Alica	Bob
vyberie náhodné $x \in \mathbb{Z}_p$	vyberie náhodné $y \in \mathbb{Z}_p$

$t_A = g^x \bmod p$ →

Dohoda na kľúči Diffie-Hellmanovou výmenou

Diffie-Hellman (1976)

veľké verejne známe prvočíslo p a generátor g grupy $\mathbb{Z}_p^*$

Alica	Bob
vyberie náhodné $x \in \mathbb{Z}_p$	vyberie náhodné $y \in \mathbb{Z}_p$

$t_A = g^x \bmod p$ →

← $t_B = g^y \bmod p$

$K = t_B{}^x \; mod \; p = g^{yx} \; mod \; p$ $\quad$ $K = t_A^y \; mod \; p = g^{xy} \bmod p$

pasívny útočník musí riešiť CDH problém $g^x, g^y \Rightarrow g^{xy}$ (mod p)

Dohoda na kľúči pomocou EC - ECDH

eliptická krivka (E, +) , generátor G ∈ E, ord(G) = q prvočíslo

Alica	Bob
vyberie $x \in \mathbb{Z}_q$	vyberie $y \in \mathbb{Z}_q$

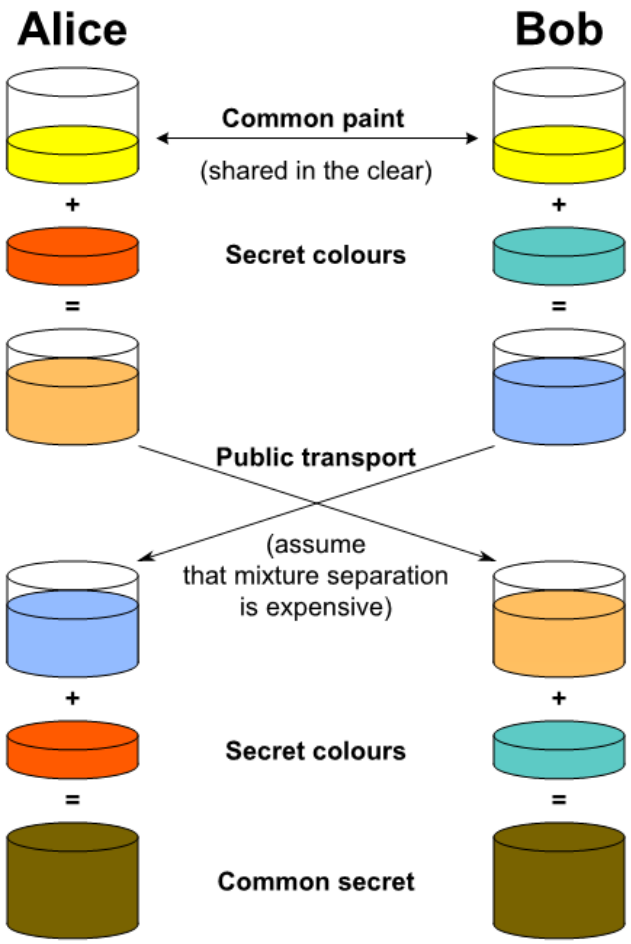
$t_A = xG$ →

← $t_B = yG$

$$K = (xt_B)_x = (xyG)_x \qquad K = (yt_A)_x = (yxG)_x$$

používa podstatne kratšie kľúče ako DH – rýchlejší výpočet

Diffie-Hellmanova výmena - ilustrácia



Man-in-the-middle útok

Alica	Cyril	Bob
vyberie $x \in \mathbb{Z}_p$	w $\in \mathbb{Z}_p$	vyberie $y \in \mathbb{Z}_p$

$t_A = g^x \bmod p$ →

$t_C = g^w \bmod p$ →

Man-in-the-middle útok

Alica	Cyril	Bob
vyberie $x \in \mathbb{Z}_p$	w $\in \mathbb{Z}_p$	vyberie $y \in \mathbb{Z}_p$

$t_A = g^x \bmod p$ →

$t_C = g^w \bmod p$ →

$t_B = g^y \bmod p$ ←

$t_C = g^w \bmod p$ ←

$$K_A = {t_C}^x \; mod \; p = g^{wx} \; mod \; p$$

$$K_B = t_C^y \; mod \; p = g^{wy} \bmod p$$

$$K_A = {t_A}^w \; mod \; p = g^{xw} \; mod \; p$$
$$K_B = {t_B}^w \; mod \; p = g^{yw} \; mod \; p$$

Man-in-the-middle útok - možná ochrana

Alica	Bob
zverejní A = g^a mod p	zverejní B = g^b mod p
vyberie náhodné $x \in \mathbb{Z}_p$	vyberie náhodné $y \in \mathbb{Z}_p$

$t_A = g^x$ mod p →

← $t_B = g^y$ mod p

$$K = t_B{}^a B^x \; mod \; p = g^{ya+bx} \; mod \; p$$

$$K = t_A^b A^y \; mod \; p = g^{xb+ay} \text{mod p}$$

A = g^a, B = g^b musia byť zverejnené bezpečným spôsobom

pre zlej implementácii

Alica	Cyril sa vydáva za Alicu
zverejní $A = g^a \bmod p$	
vyberie náhodné $x \in \mathbb{Z}_p$	vyberie náhodné $y \in \mathbb{Z}_p$

$t_A = g^x \bmod p$ →

← $t_C = t_A^{-1} g^y \bmod p$

$$K = t_C{}^a A^x \; mod \; p = g^{-xa+ya+ax} \; mod \; p$$

$$K = A^y \; mod \; p = g^{ay} \bmod p$$

ešte iný útok

Alica	Cyril	Bob
$x, x1 \in \mathbb{Z}_p$	z odpočutej relácie t_A t_B	$y, y1 \in \mathbb{Z}_p$

$t_B = g^y \bmod p$ ←

$t_A = g^x \bmod p$ →

$t'_A = g^{x1} \bmod p$ →

$t'_B = g^{y1} \bmod p$ ←

$$K_{AC} t_A'^{-c} K_{BC} t_B'^{-c} mod\ p =$$
$$= t_B{}^a C^{x1} t_A'^{-c} t_A{}^b C^{y1} t_B'^{-c} mod\ p$$
$$= g^{ya+cx1-cx1+xb+cy1-cy1}\ mod\ p$$
$$= g^{ya+bx}\ mod\ p$$

Dohoda na kľúči pomocou zdieľaného hesla

EKE – Encrypted Key Exchange (Bellowin-Merritt)

- veľké verejne známe prvočíslo p a generátor g grupy $\mathbb{Z}_p^*$
- hešované zdieľané heslo h(π)
- ra, rb – dočasné (ephemeral) kľúče A a B

A -> B : A , $E_{h(\pi)}(g^{ra} \bmod p)$ K = $f(g^{ra * rb} \bmod p)$

B -> A : $E_{h(\pi)}(g^{rb} \bmod p)$, $E_K(N_B)$

A -> B : $E_K(N_A, N_B)$

B -> A : $E_K(N_B)$

Dohoda na kľúči so zdieľaným heslom RSA výmenou

π – shared password,

ephemeral $n = p*q$, $d*e \bmod (p-1)*(q-1) = 1$

$A \rightarrow B$: $A, n, E_{h(\pi)}(e)$

$B \rightarrow A$: $E_{h(\pi)}(K^e \bmod n)$

A : $(D_{h(\pi)}(E_{h(\pi)}(K^e \bmod n)))^d \bmod n = (K^e)^d \bmod n = K$

Ďakujem za pozornosť.

jozef.jirasek@upjs.sk