Enkriptimi simetrik

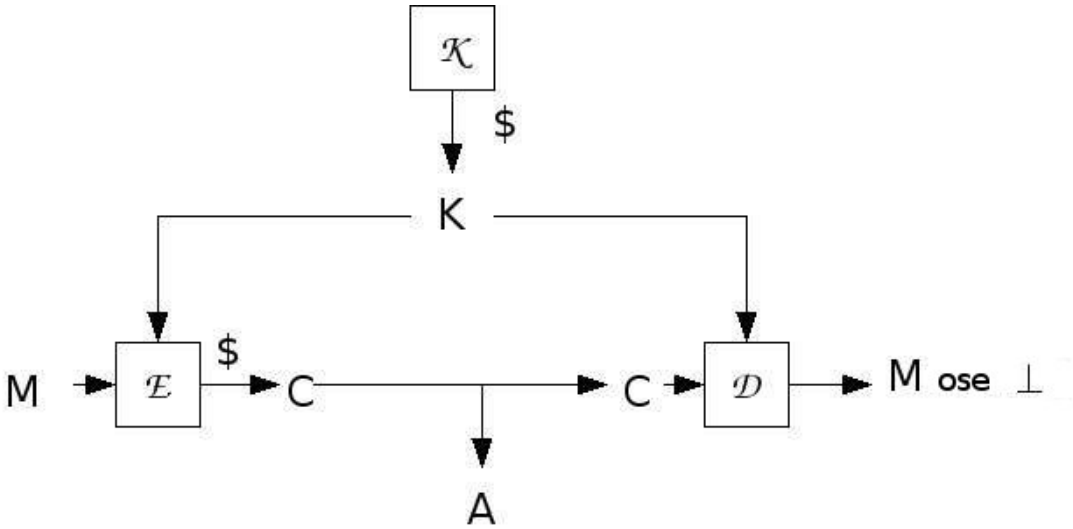
Qëllimet dhe objektivat

- Shqyrtimi i komunikimit ndërmjet dy palëve të cilat ndajnë një çelës të përbashkët.
- Zbatimi i çelësit të përbashkët për të mbrojtur të dhënat e komunikuara me atribute të ndryshme sigurie.
- Fokusimi në privatësinë e të dhënave të komunikuara, kundrejt autenticitetit të tyre.

Përmbajtja

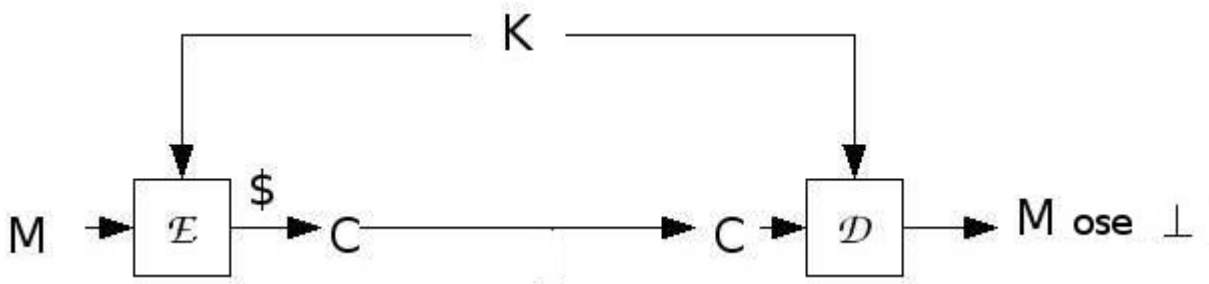
Sintaksa

- Një skemë emkriptimi simetrik $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ përbëhet nga tre algoritma:



- $\mathcal{K}$ është i rastësishëm
- $\mathcal{E}$ mund të jetë i rastësishëm ose me gjendje
- $\mathcal{D}$ është deterministik

Kërkesa e dekriptimit korrekt



- Formalisht: Për çdo çelës K dhe çdo mesazh M

$$\Pr[\mathcal{D}_K(\mathcal{E}_K(M)) = M] = 1,$$

ku probabiliteti është sipas të gjitha daljeve të $\mathcal{E}$.

Shembull: OTP

- Skema $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$, ku

$\mathcal{K}$	$\mathcal{E}_K(M)$	$\mathcal{D}_K(M)$
$K \xleftarrow{\$} \{0,1\}^k$	$C \leftarrow K \oplus M$	$M \leftarrow K \oplus C$
return K	**return** C	**return** M

- Dekriptimi korrekt

$$\begin{aligned}\mathcal{D}_K(\mathcal{E}_K(M)) &= K \oplus (K \oplus M) \\ &= (K \oplus K) \oplus M = 0^k \oplus M \\ &= M.\end{aligned}$$

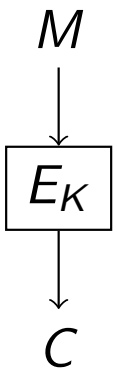
Modet e operimit blok shifrues

- Le të jetë $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ një blok shifrues
- Notacion: $x[i]$ është bloku n-bitësh i i-të i stringut x, kështu që $x = x[1] \ldots x[m]$ në qoftë se $|x| = mn$.
- Gjithmonë:

$$\frac{\mathcal{K}}{K \xleftarrow{\$} \{0,1\}^k \\ \textbf{return } K}$$

Modet e operimit blok shifrues (Vazhdim)

- Blok shifruesi pais palët që ndajnë K me



  që u mundëson të enkriptojnë mesazhe 1-blokëshe.

- Si enkriptojmë një mesazh të gjatë duke zbatuar një primitivë që zbatohet vetëm mbi bloqe n-bitëshe?

ECB: Electronic Codebook Mode

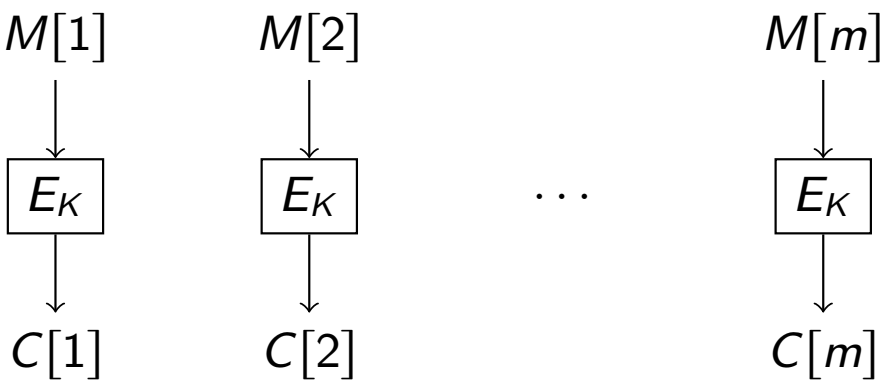
- Skema $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$, ku

$\mathcal{E}_K(M)$

for $i = 1, \ldots, m$ **do**
  $C[i] \leftarrow E_K(M[i])$
return C

$\mathcal{D}_K(C)$

for $i = 1, \ldots, m$ **do**
  $M[i] \leftarrow E_K^{-1}(C[i])$
return M



- Dekriptimi korrekt mbështetet mbi faktin se E është blok shifures, kështu që E_K është i invertueshëm.

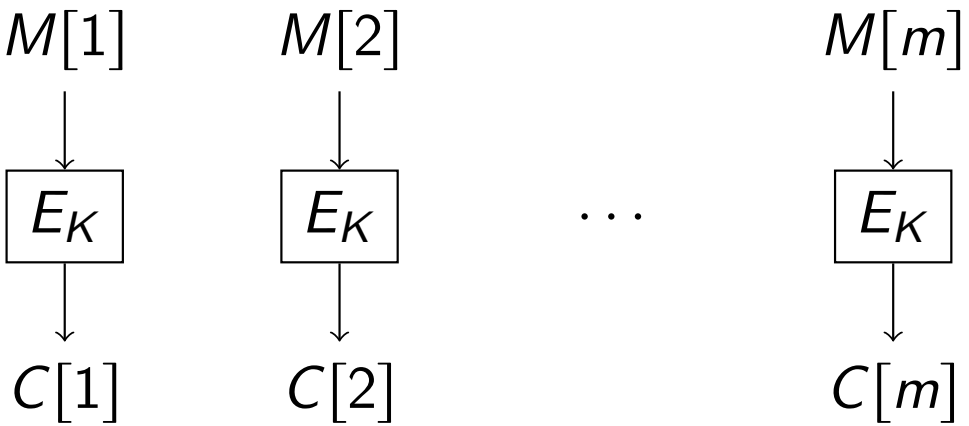
Vlerësimi i sigurisë

- Dërguesi enkripton disa mesazhe $M_1, \ldots, M_q$, d.m.th.

$$C_1 \leftarrow \mathcal{E}_K(M_1), \ldots, C_q \leftarrow \mathcal{E}_K(M_q)$$

  dhe i dërgon $C_1, \ldots, C_q$ pranuesit.
- Kundërshtari
  - Di $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$
  - Di $C_1, \ldots, C_q$
  - **Nuk** e ka çelësin K!
- Qëllimet e mundshme të kundërshtarit:
  - Kthe K
  - Kthe M_1
- Por na duhet të shikojmë përtej këtyre

Siguria e ECB

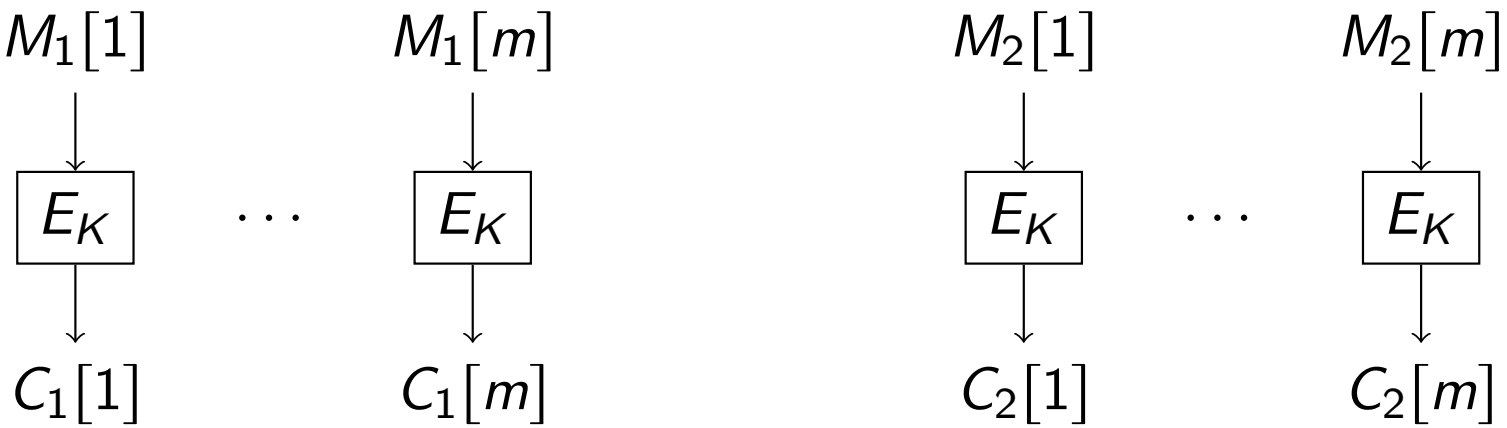


- Kundërshtari ka tekstin e shifruar $C = C[1] \dots C[m]$

Detyra e kundërshtarit	Vlerësimi	Pse?
Llogarit K	Duket vështirë	E i sigurt
Llogarit $M[1]$	Duket vështirë	E i sigurt

Siguria e ECB (Vazhdim)

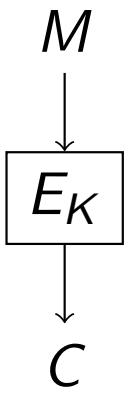
- Dobësi: $M_1 = M_2 \implies C_1 = C_2$
- Pse është kështu? Sepse E_K është deterministik:



- Pse është kjo e rëndësishme?

Siguria e ECB (Vazhdim)

- Supozojmë se dijmë se ekzistojnë vetëm dy mesazhe të mundshme, $Y = 1^n$ dhe $N = 0^n$, që paraqesin, për shembull,
  - Voto PO ose JO
  - BLEJ ose SHIT një letër me vlerë
  - SHKREP ose MOS SHKREP një predhë
- ECB algoritmi do të jetë $\mathcal{E}_K(M) = E_K(M)$.



Siguria e ECB (Vazhdim)

- Votat $M_1, M_2 \in \{ Y, N\}$ janë ECB të enkriptuara dhe kundërshtari sheh tekstin e shifruar $C_1 = E_K(M_1)$ dhe $C_2 = E_K(M_2)$.

- Kundërshtari mund të ketë hedhur votën e parë, dhe kështu të dijë M_1; të themi $M_1 = Y$. Atëherë kundërshtari mund të gjejë M_2:
  - Në qoftë se $C_2 = C_1$, atëherë $M_2 = Y$
  - Përndryshe $M_2 = N$

A mund të evitohet pasiguria e ECB

- Le të jetë $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ një skemë enkriptimi **e çfarëdoshme**.
- Supozojmë se $M_1, M_2 \in \{ Y, N \}$ dhe
  - Dërguesi dërgon tekstet e shifruara $C_1 = \mathcal{E}_K(M_1)$ dhe $C_2 = \mathcal{E}_K(M_2)$
  - Kundërshtari $\mathcal{A}$ di se $M_1 = Y$.

  janë ECB të enkriptuara dhe kundërshtari sheh tekstin e shifruar $C_1 = E_K(M_1)$ dhe $C_2 = E_K(M_2)$.
- Kundërshtari $\mathcal{A}$:

$\mathcal{A}$

---

if $C_2 = C_1$ **then** $M_2 \leftarrow Y$

else $M_2 \leftarrow N$

return M_2

- A funksionon sulmi i tillë?
- Po, në qoftë se $\mathcal{E}$ është deterministik.

Enkriptimi i rastësishëm

- Që të jetë i sigurt enkriptimi duhet të jetë i rastësishëm.
- D.m.th., algoritmi $\mathcal{E}_K$ „hedh metelikë“.
- Në qoftë se i njëjti mesazh enkriptohet dy herë ka të ngjarë që marrim tekste të shifruara të ndryshme. D.m.th., në qoftë se $M_1 = M_2$ dhe

$$C_1 \xleftarrow{\$} \mathcal{E}_K(M_1) \quad \text{dhe} \quad C_2 \xleftarrow{\$} \mathcal{E}_K(M_2),$$

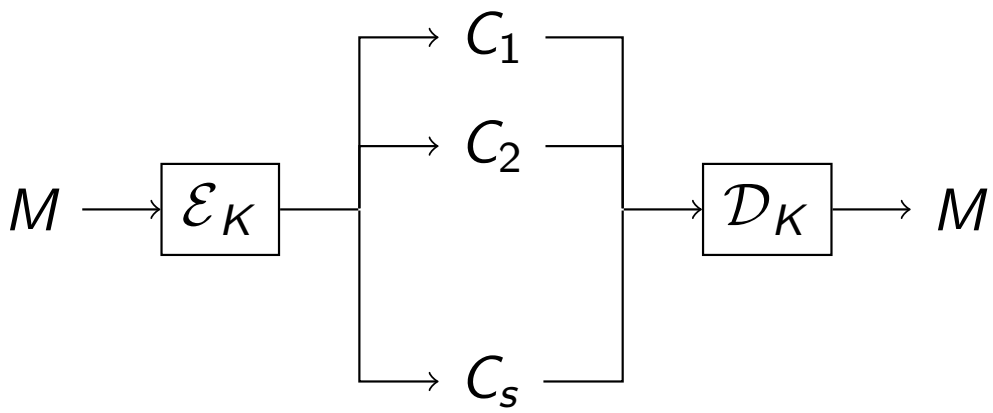
atëherë

$$\Pr[C_1 = C_2]$$

do të (duhet të) jetë i vogël, ku probabiliteti është sipas metelikëve të $\mathcal{E}$.

Enkriptimi i rastësishëm (Vazhdim)

- Ka shumë tekste të shifruara të mundshme që i korrespondojnë secilit mesazh.
- Atëherë, si mund të dekriptojmë?
- Do të shohim shembuj së shpejti.



Enkriptimi i rastësishëm (Vazhdim)

- Një zhvendosje fundamentale nga nocionet klasike dhe konvencionale të enkriptimit
- Tradicionalisht, enkriptimi (p.sh., shifruesi me zëvendësim) është kod që çdo mesazhi i asocon një tekst të shifruar unik.
- Tani po themi se asnjë kod i tillë nuk është i sigurt, dhe po kërkojmë për mekanizëm enkriptimi i cili i asocon një mesazhi një numër tekstesh të shifruara të ndryshme.

Enkriptimi me gjendje

- Një alternativë e enkriptimim të rastësishëm është t'i lejohet algoritmit të enkriptimit të mbajë gjendjen. Kjo mund të jetë një numërues.
  - Enkripto varësisht nga gjendja e numëruesit
  - Pastaj azhorno numëruesin
- Do të shqyrtojmë skema që përdorin këtë paradigmë për të tejkaluar dobësitë e sigusisë të enkriptimit deterministik.

Disa mode tjera operimi

- Mode operimi me enkriptim të rastësishëm:
  - CBC$
  - CTR$
- Mode operimi me enkriptim me gjendje:
  - CBCC
  - CTRC

CBC$: Cipher Block Chaining me modin e rastësishëm IV

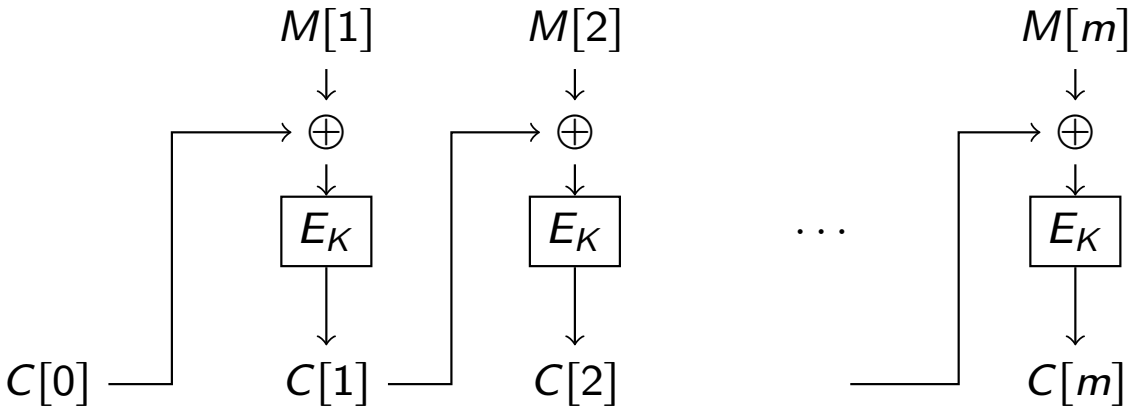
- Skema $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$, ku

$\mathcal{E}_K(M)$

$C[0] \xleftarrow{\$} \{0,1\}^n$
for $i = 1, \ldots, m$ **do**
  $C[i] \leftarrow E_K(M[i] \oplus C[i-1])$
return C

$\mathcal{D}_K(C)$

for $i = 1, \ldots, m$ **do**
  $M[i] \leftarrow E_K^{-1}(C[i]) \oplus C[i-1]$
return M



- Dekriptimi korrekt mbështetet mbi faktin se E është blok shifures, kështu që E_K është i invertueshëm.

CTRC modi

- Dërguesi mban një numërues *ctr* që inicializohet në 0 dhe azhornohet nga $\mathcal{E}$.
- Shënojmë me $< j >$ paraqitjen n-bitëshe të numrit të plotë j $(0 \leqslant j \leqslant 2^n)$.

$\mathcal{E}_K(M)$

$C[0] \leftarrow ctr$

for $i = 1, \ldots, m$ **do**

$P[i] \leftarrow E_K(< ctr + i >)$

$C[i] \leftarrow P[i] \oplus M[i]$

return C

$\mathcal{D}_K(C)$

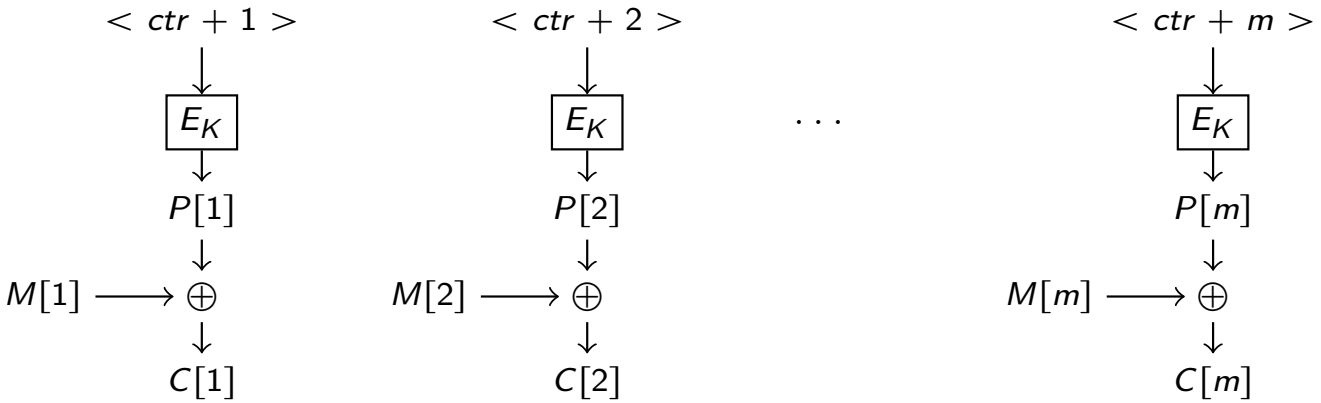
$ctr \leftarrow C[0]$

for $i = 1, \ldots, m$ **do**

$P[i] \leftarrow E_K(< ctr + i >)$

$M[i] \leftarrow P[i] \oplus C[i]$

return M



CTRC modi (Vazhdim)

$\mathcal{E}_K(M)$

$C[0] \leftarrow ctr$
for $i = 1, \ldots, m$ **do**
  $P[i] \leftarrow E_K(< ctr + i >)$
  $C[i] \leftarrow P[i] \oplus M[i]$
return C

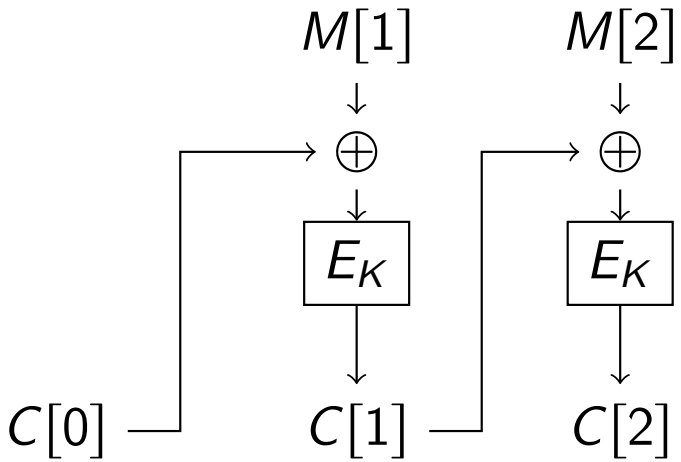
$\mathcal{D}_K(C)$

$ctr \leftarrow C[0]$
for $i = 1, \ldots, m$ **do**
  $P[i] \leftarrow E_K(< ctr + i >)$
  $M[i] \leftarrow P[i] \oplus C[i]$
return M

- Dekriptuesi nuk mban numërues.
- $\mathcal{D}$ nuk përdor E_K^{-1}!
- Enkritptimi dhe dekriptimi janë të paralelizueshëm.

Siguria e CBC$ kundrejt kthimit të çelësit

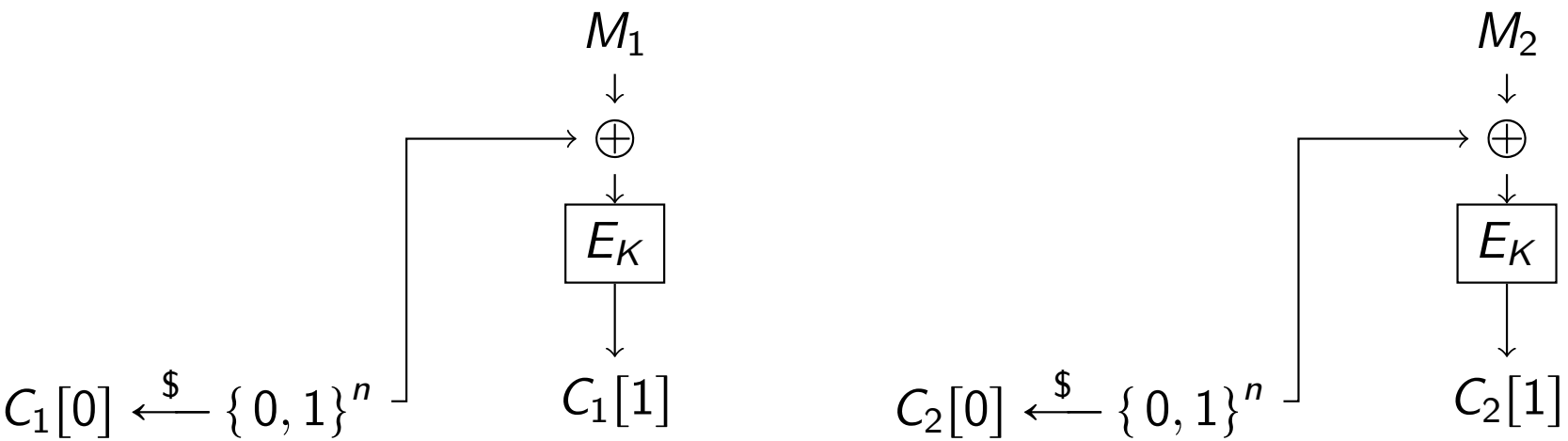
- Në qoftë se kundërshtari ka një tekst mesazhi M dhe tekstin e shifruar përkatës $C \xleftarrow{\$} \mathcal{E}_K(M)$, atëherë ai ka shembuj hyrje/dalje $(M[1] \oplus C[0], C[1])$, $(M[2] \oplus C[1], C[2])$ të E_K



- Kështu, mund të ngritet sulme të mesazhit të zgjedhur për kthim çelësi mbi E për të kthyer K.
- **Përfundimi:** Siguria e CBS$ kundrejt kthimit të çelësit nuk është më e mirë sesa ajo e blok shifruesit mbi të cilin mbështet.

Votimi me CBC$

- Supozojmë se enkriptojmë $M_1, M_2 \in \{Y, N\}$ me CBC$.



- Kundërshtari $\mathcal{A}$ sheh $C_1 = C_1[0]C_1[1]$ dhe $C_2 = C_2[0]C_2[1]$.
- Supozojmë se $\mathcal{A}$ di se $M_1 = Y$.
- A mund të përcaktojë $\mathcal{A}$ se a është $M_2 = Y$ apo $M_2 = N$?
- **Jo!**

Votimi me CBC$ (Vazhdim)

- Në qoftë se $M_1 = Y$, kemi

- $\mathcal{A}$ di $C_1[0]C_1[1]$ dhe $C_2[0]C_2[1]$.
  - Në qoftë se $C_1[0] = C_2[0]$, atëherë $\mathcal{A}$ mund të konkludojë se
    - Në qoftë se $C_2[1] = C_1[1]$, atëherë $M_2 = Y$
    - Në qoftë se $C_2[1] \neq C_1[1]$, atëherë $M_2 = N$
  - Por, probabiliteti që $C_1[0] = C_2[0]$ është shumë i vogël.

Vlerësimi i sigurisë

- Kështu, CBC$ është më i mirë se ECB. Por a është i sigurt?
- CBC$ është skema e enkriptimit më të shfrytëzuar në botë (SSL, SSH, TLS, ...), kështu që është me rëndësi të dihet se a është e sigurt.
- Për t'u përgjegjur duhet më parë të vendosim dhe të formalizojmë çfarë nënkuptojmë me siguri?

Tipet e skemave të enkriptimit

- *Me destinim të posaçëm:* Përdoren në konfigurim specifik, për të enkriptuar të dhëna të ndonjë formati ose shpërndarjeje të njohur.
  - **Kujdes!** Të përdoret vetëm nën kushtet X.
- *Me destinim të përgjithshëm:* Përdoren për enkriptim në shumë konfigurime të ndryshme, ku formati i të dhënave dhe shpërndajra e tyre nuk janë të njohura paraprakisht.
- Na duhen skemat me destinim të përgjithshëm sepse
  - Mund të standardizohen dhe të përdoren gjerë
  - Kur një skemë të dalë njëherë, përdoret për gjithçka sidoqoftë
  - Skemat me destinim të përgjithshëm përdoren më lehtë dhe keçpërdoren më vështirë: është e vështirë për disenjuesit e aplikacioneve të dijnë se a plotësohet kushti X.

Kërkesat e sigurisë

- Informatat apriori: Çfarë di tanimë kundërshtari mbi të dhënat nga konteksti. P.sh., se mesazhet janë njëra nga $\{Y, N\}$.
- Shpërndarja ose formati i të dhënave: Të dhënat mund të jenë në gjuhën angleze ose jo; mund të kenë komponentë rastësie ose jo; ...
- Siguria nuk duhet të mbështetet në supozime të tilla.

Enkriptimi i e-mail-it

- Një email mund të jetë
  - Tekst në gjuhën shqipe
  - Tekst në gjuhën angleze
  - Fajl pdf ose ekzekutues
  - Votë
- Kërkohet siguri në të gjitha këto raste

Kërkesat e sigurisë (Vazhdim)

- Supozojmë se dërguesi kompjuton

$$C_1 \xleftarrow{\$} \mathcal{E}_K(M_1), \ldots, C_q \xleftarrow{\$} \mathcal{E}_K(M_q).$$

- Kundërshtari $\mathcal{A}$ ka $C_1, C_2, \ldots, C_q$.

Në qoftë se $\mathcal{A}$	
Kthen K	Keç!
Kthen M_1	Keç!

- Por poashtu...

Kërkesat e sigurisë (Vazhdim)

- Duam t'i fshehim të gjitha informatat parciale mbi rrjedhën e të dhënave.
- Shembuj informatash parciale:
  - A është $M_1 = M_2$?
  - Cili është biti i parë i M_1?
  - Cili XOR i bitëve të parë të M_1, M_2?
- Diçka që nuk fshehim dot: gjatësia e mesazhit.

Çfarë kërkojmë

- Duam një veti të veçantë „master“ VM të një skeme enkriptimi të tillë që
  - VM mund të specifikohet lehtë
  - Mund të vlerësojmë se a e plotëson skema VM
  - VM implikon të gjitha kushtet e sigurisë që i dëshirojmë: Garanton se një tekst i shifruar nuk zbulon **asnjë** informatë parciale mbi mesazhin.
- Kështu, një semë që ka VM jo vetëm që implikon se në qoftë se kundërshtari ka $C_1 \xleftarrow{\$} \mathcal{E}_K(M_1)$ dhe $C_2 \xleftarrow{\$} \mathcal{E}_K(M_2)$, atëherë
  - Ai nuk mund të gjejë M_1
  - Ai nuk mund të gjejë bitin e parë të M_1?
  - Ai nuk numd të gjejë XOR të bitëve të parë të M_1, M_2,

  por, në fakt, implikon se të gjitha informatat e tilla mbi M_1, M_2 janë të mbrojtura.

Kërkimi i VM

- Atëherë, çfarë është veti master VM?
- Është nocion i quajtur *padallueshmëri* (*indistinguishability*, IND). Do t'i përkufizojmë
  - IND-CPA: Padallueshmëria nën sulmin e mesazhit të zgjedhur (chosen-plaintext attack)
  - IND-CCA: Padallueshmëria nën sulmin e tekstit të shifruar të zgjedhur (chosen-ciphertext attack)

Plani

- Përkufizojmë IND-CPA
- Shembuj skemash që nuk janë IND-CPA
- Shqyrtojmë pse IND-CPA është VM, d.m.th. pse implikon se tekstet e shifruara nuk rrjedhin asnjë inormatë parciale mbi tekstet e shifruara.
- Shembuj skemash që janë IND-CPA
- IND-CCA

Intuita për përkufizimin e IND

- Shqyrtojmë enkriptimin e njërës nga dy rrjedhat e mundshme të dhënash: ose

$$M_0^1, \ldots, M_0^q$$

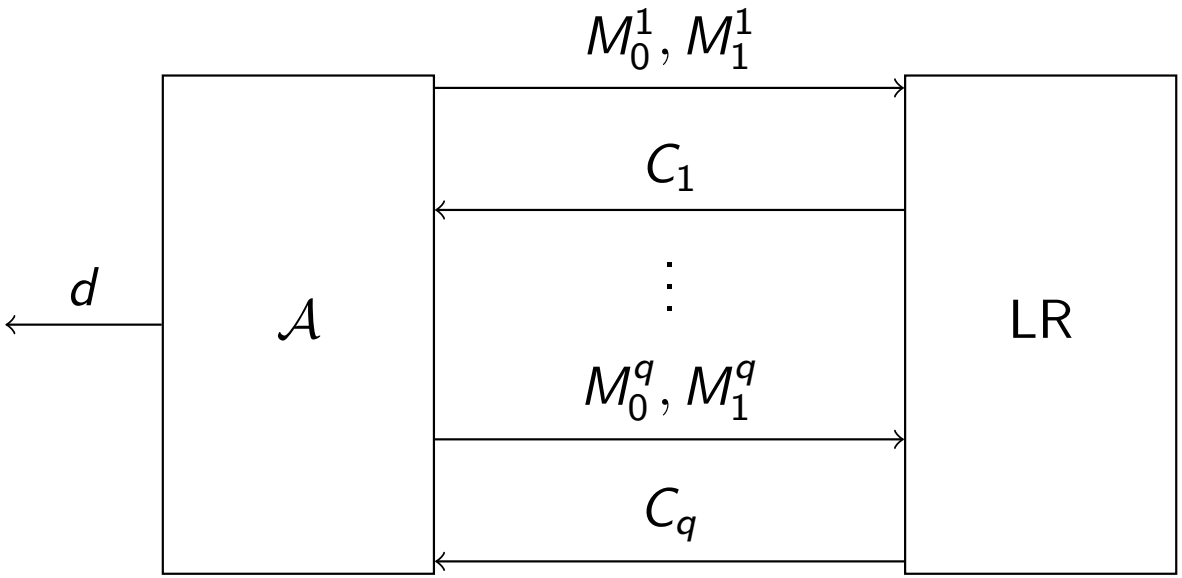
ose

$$M_1^1, \ldots, M_1^q$$

- Kundërshtari, i cili posedon tekstin e shifruar dhe të dyja rrjedhat e të dhënave, duhet të gjejë se cila nga të dyja rrjedhat është enkriptuar.

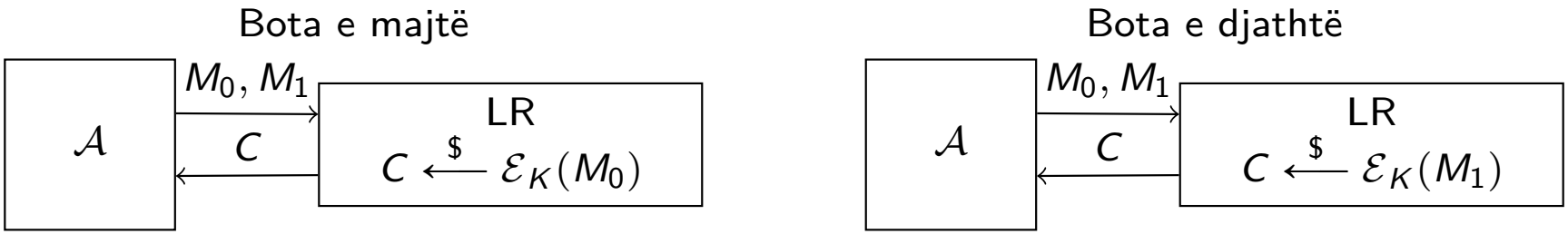
ind-cpa-kundërshtarët

- Le të jetë $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ një skemë enkriptimi.
- Një ind-cpa-kundërshtar $\mathcal{A}$ ka një orakul LR
  - Mund të bëjë një pyetësor M_0, M_1 i cili përbëhet nga çfarëdo mesazhesh me gjatësi të barabarta
  - Mund të bëjë këtë shumë herë
  - Secilën herë merr në kthim tekst të shifruar
  - Më në fund ai jep një bit në dalje.



ind-cpa-kundërshtarët (Vazhdim)

- Le të jetë $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ një skemë enkriptimi.



Dalja d e $\mathcal{A}$	Domethënia e dëshiruar: Mendoj se jam në
1	Botën e djathtë
0	Botën e majtë

- Sa më vështirë të jetë për $\mathcal{A}$ që ta qëllojë se në cilën botë ndodhet, aq „më e sigurt“ është $\mathcal{SE}$ si skemë enkriptuese.

Lojërat

- Le të jetë $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ një skemë enkriptimi.

Loja $\text{Left}_{\mathcal{SE}}$

$K \xleftarrow{\$} \mathcal{K}$

$\text{LR}(M_0, M_1)$

return $C \xleftarrow{\$} \mathcal{E}_K(M_0)$

Loja $\text{Right}_{\mathcal{SE}}$

$K \xleftarrow{\$} \mathcal{K}$

$\text{LR}(M_0, M_1)$

return $C \xleftarrow{\$} \mathcal{E}_K(M_1)$

- $\mathcal{SE}$ dhe $\mathcal{A}$ u shoqërohen probabilitetet

$$\Pr\left[\text{Left}^{\mathcal{A}}_{\mathcal{SE}} = 1\right] \quad \text{dhe} \quad \Pr\left[\text{Right}^{\mathcal{A}}_{\mathcal{SE}} = 1\right]$$

që $\mathcal{A}$ jep 1 në dalje në secilën botë.

- *ind-cpa-përparsia* e $\mathcal{A}$ është

$$\text{Adv}^{\text{ind}-\text{cpa}}_{\mathcal{SE}}(\mathcal{A}) = \Pr\left[\text{Right}^{\mathcal{A}}_{\mathcal{SE}} = 1\right] - \Pr\left[\text{Left}^{\mathcal{A}}_{\mathcal{SE}} = 1\right].$$

Shembull

- Le të jetë $E : \{0,1\}^k \times \{0,1\}^{128} \to \{0,1\}^{128}$ një blok shifrues dhe $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ skema e enkriptimit e përkufizuar me

$\mathcal{K}$	$\mathcal{E}_K(M)$	$\mathcal{D}_K(C)$
$K \xleftarrow{\$} \mathcal{K}$	**return** $E_K(M)$	**return** $E_K^{-1}(C)$
return K		

- Kjo skemë enkripton vetëm mesazhe 1-blokëshe.
- Përmbledhur: $\mathcal{E}_K(M) = E_K(M)$.

Shembull (Vazhdim)

- Le të jetë $\mathcal{E}_K(M) = E_K(M)$ dhe le të jetë $\mathcal{A}$ kundërshtari vijues

  $\mathcal{A}$

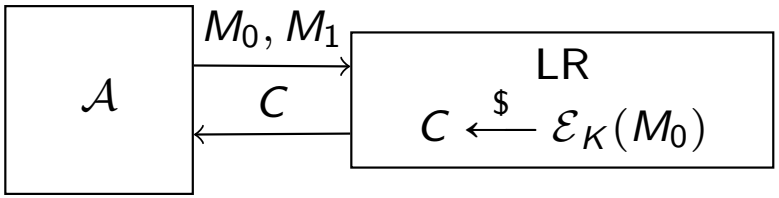
  $C_1 \leftarrow \mathrm{LR}(0^n, 0^n)$

  $C_2 \leftarrow \mathrm{LR}(1^n, 0^n)$

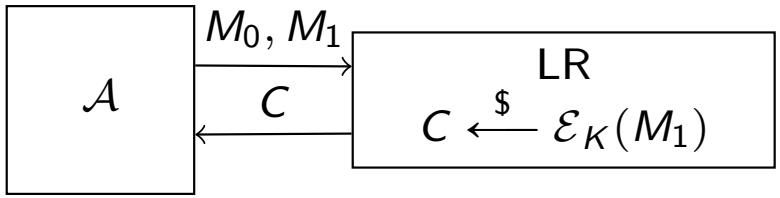
  if $C_1 = C_2$ **then return** 1

  else return 0

Bota e majtë



Bota e djathtë



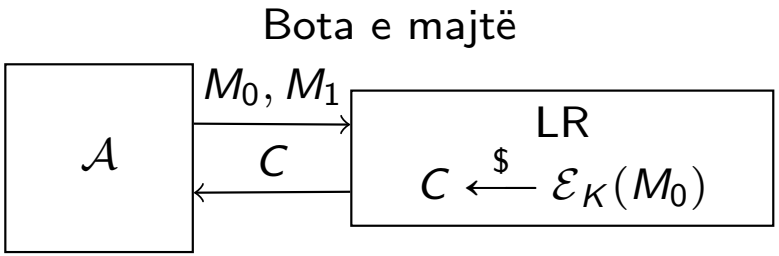
- Atëherë,

$$\Pr[\mathrm{Left}^{\mathcal{A}}_{\mathcal{SE}} = 1] = ?$$

$$\Pr[\mathrm{Right}^{\mathcal{A}}_{\mathcal{SE}} = 1] = ?$$

Shembull (Vazhdim)

- Le të jetë $\mathcal{E}_K(M) = E_K(M)$.



$\mathcal{A}$

$C_1 \leftarrow \mathrm{LR}(0^n, 0^n)$

$C_2 \leftarrow \mathrm{LR}(1^n, 0^n)$

if $C_1 = C_2$ **then return** 1

else return 0

- Çfarë ndodh
  - $C_1 = \mathcal{E}_K(0^n) = E_K(0^n)$
  - $C_2 = \mathcal{E}_K(1^n) = E_K(1^n) \neq E_K(0^n)$
  - Prandaj $C_1 \neq C_2$ dhe $\mathcal{A}$ kthen 0
- Kështu

$$\Pr[\mathrm{Left}^{\mathcal{A}}_{\mathcal{SE}} = 1] = 0$$

Shembull (Vazhdim)

- Le të jetë $\mathcal{E}_K(M) = E_K(M)$.

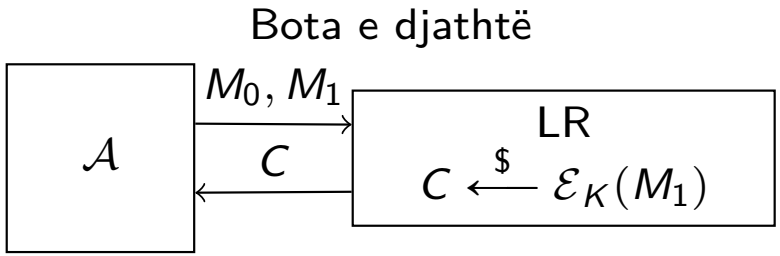
$\mathcal{A}$

$C_1 \leftarrow \mathrm{LR}(0^n, 0^n)$

$C_2 \leftarrow \mathrm{LR}(1^n, 0^n)$

if $C_1 = C_2$ **then return** 1

else return 0



- Çfarë ndodh
  - $C_1 = \mathcal{E}_K(0^n) = E_K(0^n)$
  - $C_2 = \mathcal{E}_K(0^n) = E_K(0^n)$
  - Prandaj $C_1 = C_2$ dhe $\mathcal{A}$ kthen 1
- Kështu

$$\Pr[\mathrm{Right}^{\mathcal{A}}_{\mathcal{SE}} = 1] = 1$$

Shembull (Vazhdim)

- Le të jetë $\mathcal{E}_K(M) = E_K(M)$.

$\mathcal{A}$

$C_1 \leftarrow \mathsf{LR}(0^n, 0^n)$

$C_2 \leftarrow \mathsf{LR}(1^n, 0^n)$

if $C_1 = C_2$ **then return** 1

else return 0

$$\begin{aligned}\mathsf{Adv}^{\mathrm{ind-cpa}}_{\mathcal{SE}}(\mathcal{A}) &= \Pr[\mathsf{Right}^{\mathcal{A}}_{\mathcal{SE}} = 1] - \Pr[\mathsf{Left}^{\mathcal{A}}_{\mathcal{SE}} = 1] \\ &= 1 - 0 = 1\end{aligned}$$

Masa e suksesit

- Le të jetë $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ një skemë enkriptimi dhe le të jetë $\mathcal{A}$ një ind-cpa kundërshtar.
- Atëherë,

$$\mathsf{Adv}^{\mathrm{ind-cpa}}_{\mathcal{SE}}(\mathcal{A}) = \Pr[\mathsf{Right}^{\mathcal{A}}_{\mathcal{SE}} = 1] - \Pr[\mathsf{Left}^{\mathcal{A}}_{\mathcal{SE}} = 1]$$

  është numër ndërmjet -1 dhe 1.
- Përparsi „e madhe“ (afër 1) do të thotë
  - $\mathcal{A}$ është duke shkuar mirë
  - $\mathcal{SE}$ nuk është i sigurt
- Përparsi „e vogël“ (afër 0 ose $\leqslant 0$) do të thotë
  - $\mathcal{A}$ është duke shkuar dobët
  - $\mathcal{SE}$ i reziston sulmeve të ngirtura nga $\mathcal{A}$

Siguria IND-CPA

- Përparsia e kundërshtarit varet nga
  - strategjia e tij
  - resurset: kompleksiteti kohor t dhe numri q i orakul pyetësorëve
- **Siguria:** $\mathcal{SE}$ është *IND-CPA* (i sigurt) në qoftë se $\mathrm{Adv}^{\mathrm{ind-cpa}}_{\mathcal{SE}}(\mathcal{A})$ është „e vogël“ për **çdo** $\mathcal{A}$ që shfrytëzon sasi „praktike“ resursesh.

Shembull

Siguria 80-bitëshe do të mund të përkufizohej ashtu që për çdo $n = 1, \ldots, 80$ të kemi

$$\mathrm{Adv}^{\mathrm{ind-cpa}}_{\mathcal{SE}}(\mathcal{A}) \leqslant 2^{-n}$$

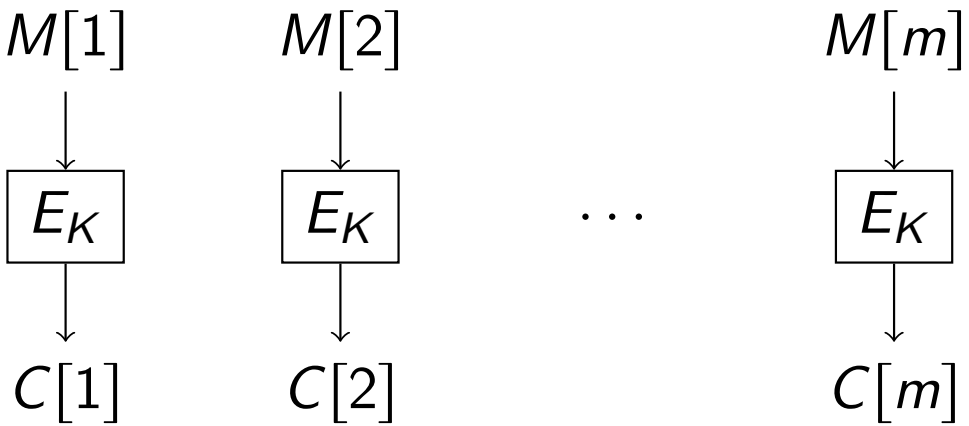
për çdo $\mathcal{A}$ me kompleksitet kohor dhe numër orakul pyetësorësh të shumtën 2^{80-n}.

- **Pasiguria:** $\mathcal{SE}$ nuk është IND-CPA (i sigurt) në qoftë se ekziston $\mathcal{A}$ i cili përdor „pak“ resurse që arrin përparsi „të madhe“.

ECB nuk është IND-CPA i sigurt

- Le të jetë $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ një blok shifrues. Rikujtojmë se ECB modi përkufizon skemën simetrike të enkriptimit $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ me

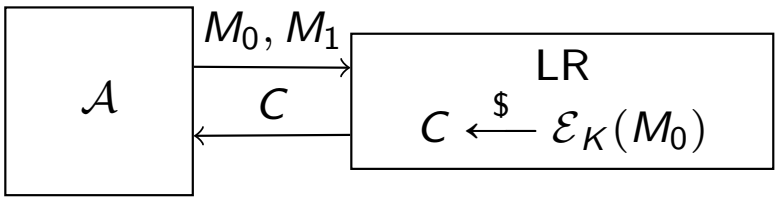
$$\mathcal{E}_K(M) = E_K(M[1])E_K(M[2])\ldots E_K(M[m])$$



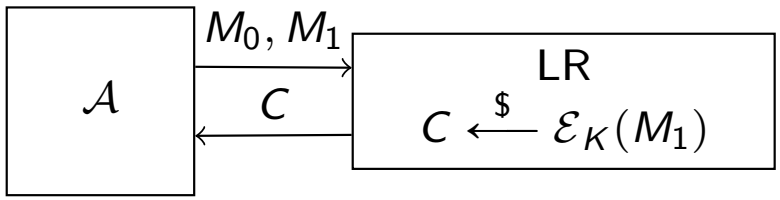
ECB nuk është IND-CPA i sigurt (Vazhdim)

- Le të jetë $\mathcal{E}_K(M) = E_K(M[1])E_K(M[2])\ldots E_K(M[m])$.

Bota e majtë



Bota e djathtë



- A mund të disenjojmë $\mathcal{A}$ ashti që

$$\mathsf{Adv}^{\mathrm{ind-cpa}}_{\mathcal{SE}}(\mathcal{A}) = \Pr[\mathsf{Right}^{\mathcal{A}}_{\mathcal{SE}} = 1] - \Pr[\mathsf{Left}^{\mathcal{A}}_{\mathcal{SE}} = 1]$$

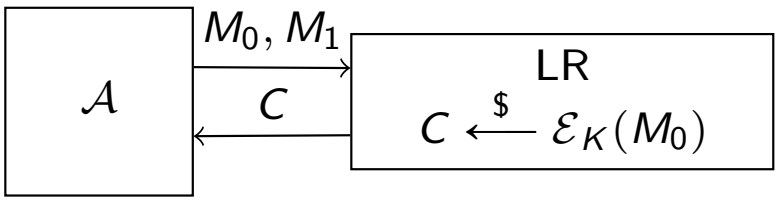
  të jetë afër 1?
- Dobësi e $\mathcal{SE}$ që mund të shfrytëzohet:

$$M_1 = M_2 \implies \mathcal{E}_K(M_1) = \mathcal{E}_K(M_2)$$

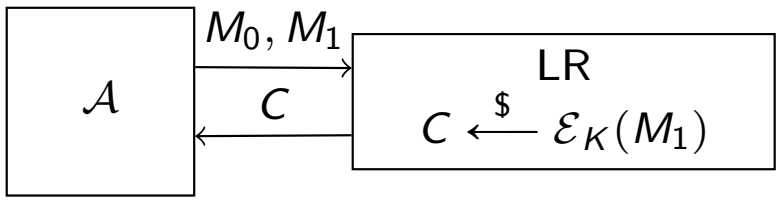
ECB nuk është IND-CPA i sigurt (Vazhdim)

- Le të jetë $\mathcal{E}_K(M) = E_K(M[1])E_K(M[2])\ldots E_K(M[m])$.

Bota e majtë



Bota e djathtë



$\mathcal{A}$

$C_1 \leftarrow \mathrm{LR}(0^n, 0^n)$

$C_2 \leftarrow \mathrm{LR}(1^n, 0^n)$

if $C_1 = C_2$ **then return** 1

else return 0

ECB nuk është IND-CPA: Analiza e botës së majtë

- Le të jetë $\mathcal{E}_K(M) = E_K(M[1])E_K(M[2])\ldots E_K(M[m])$.

$\mathcal{A}$

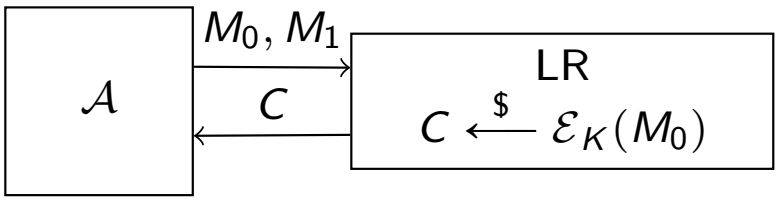
$C_1 \leftarrow \mathrm{LR}(0^n, 0^n)$

$C_2 \leftarrow \mathrm{LR}(1^n, 0^n)$

if $C_1 = C_2$ **then return** 1

else return 0

Bota e majtë



Loja $\mathrm{Left}_{\mathcal{SE}}$

$K \xleftarrow{\$} \mathcal{K}$

$\mathrm{LR}(M_0, M_1)$

---

return $C \xleftarrow{\$} \mathcal{E}_K(M_0)$

- Atëherë,

$$\Pr[\mathrm{Left}^{\mathcal{A}}_{\mathcal{SE}} = 1] = 0$$

sepse $C_1 = E_K(0^n) \neq E_K(1^n) = C_2$.

ECB nuk është IND-CPA: Analiza e botës së djathtë

- Le të jetë $\mathcal{E}_K(M) = E_K(M[1])E_K(M[2])\ldots E_K(M[m])$.

$\mathcal{A}$

$C_1 \leftarrow \mathrm{LR}(0^n, 0^n)$; $C_2 \leftarrow \mathrm{LR}(1^n, 0^n)$

if $C_1 = C_2$ **then return** 1

else return 0

Loja $\mathrm{Right}_{\mathcal{SE}}$

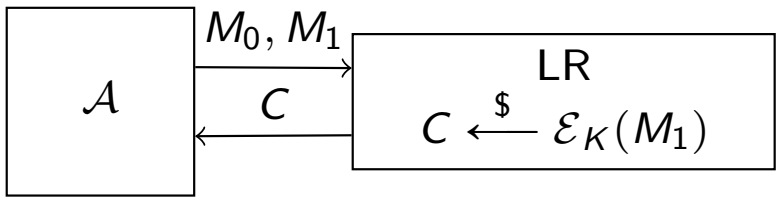
$K \xleftarrow{\$} \mathcal{K}$

$\mathrm{LR}(M_0, M_1)$

---

return $C \xleftarrow{\$} \mathcal{E}_K(M_1)$

Bota e djathtë



- Atëherë,

$$\Pr[\mathrm{Left}^{\mathcal{A}}_{\mathcal{SE}} = 1] = 1$$

sepse $C_1 = E_K(0^n) = E_K(0^n) = C_2$.

ECB nuk është IND-CPA i sigurt (Vazhdim)

$\mathcal{A}$

$C_1 \leftarrow \mathsf{LR}(0^n, 0^n); C_2 \leftarrow \mathsf{LR}(1^n, 0^n)$

if $C_1 = C_2$ **then return** 1

else return 0

$$\begin{aligned}\mathsf{Adv}^{\mathrm{ind-cpa}}_{\mathcal{SE}}(\mathcal{A}) &= \Pr[\mathsf{Right}^{\mathcal{A}}_{\mathcal{SE}} = 1] - \Pr[\mathsf{Left}^{\mathcal{A}}_{\mathcal{SE}} = 1] \\ &= 1 - 0 = 1\end{aligned}$$

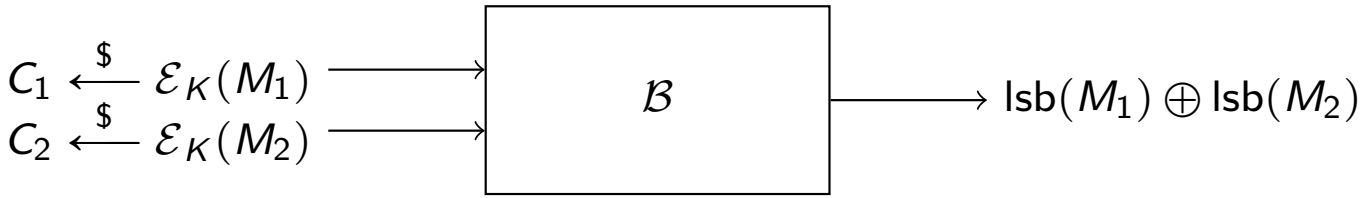
- $\mathcal{A}$ është shumë efikas, duke bërë vetëm 2 pyetësorë.
- Kështu, ECB **nuk** është IND-CPA i sigurt.

Pse IND-CPA është veti „master“ (VM)?

- Pohojmë se në qoftë se një skemë enkriptimi $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ është IND-CPA e sigurt, atëherë teksti i shifruar fsheh të gjitha informatat parciale mbi tekstin e mesazhit.
- Për shembull, mga $C_1 \xleftarrow{\$} \mathcal{E}_K(M_1)$ dhe $C_2 \xleftarrow{\$} \mathcal{E}_K(M_2)$ kundërshtari nuk mund të
  - gjejë M_1
  - gjejë bitin e parë të M_1
  - gjejë XOR të bitëve të parë të M_1, M_2
  - etj.
- Pse është ky pohim i vërtetë?

XOR-pasiguria implikon IND-CPA-pasigurinë

- Le të jetë $\mathsf{lsb}(M)$ biti i fundit i M.
- Supozojmë se është dhënë një kundërshtar $\mathcal{B}$ i tillë që



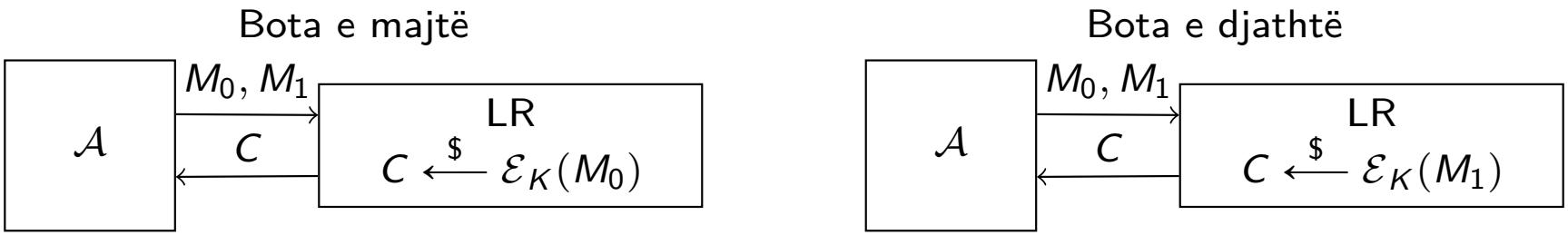
  për çdo M_1, M_2.
- Pohojmë se mund të disenjojmë një ind-cpa kundërshtar $\mathcal{A}$ të tillë që

$$\mathsf{Adv}^{\mathrm{ind-cpa}}_{\mathcal{SE}}(\mathcal{A}) = 1,$$

  që d.m.th. se $\mathcal{SE}$ nuk është IND-CPA i sigurt.
- Kështu,

$$\text{XOR-pasiguria} \implies \text{IND-CPA-pasigurinë}$$
$$\text{IND-CPA-siguria} \implies \text{XOR-sigurinë}$$

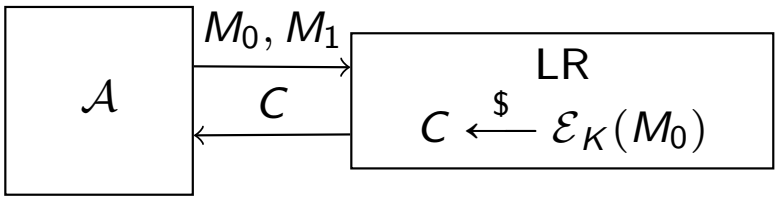
XOR-pasiguria implikon IND-CPA-pasigurinë (Vazhdim)



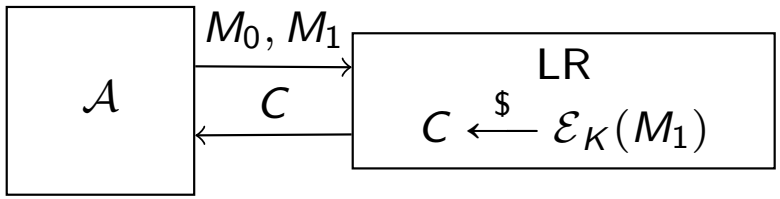
- Kundërshtari $\mathcal{A}$
  - Bën dy LR pyetësorë
  - Mesazhet e majta janë $M_0^1 = 0^n$ dhe $M_0^2 = 0^n$.
    - Pse? Sepse $\mathsf{lsb}(0^n) \oplus \mathsf{lsb}(0^n) = 0$
  - Mesazhet e djathta janë $M_1^1 = 0^n$ dhe $M_1^2 = 1^n$.
    - Pse? Sepse $\mathsf{lsb}(0^n) \oplus \mathsf{lsb}(1^n) = 1$
  - Merr dy tekstet e shifruara C_1, C_2.
  - Ekzekuton $\mathcal{B}(C_1, C_2)$ për të llogaritur $\mathsf{lsb}(M_d) \oplus \mathsf{lsb}(M_d)$, që është e barabartë me d, duke indikuar ose botën e majtë ose të djathtën.

XOR-pasiguria implikon IND-CPA-pasigurinë (Vazhdim)

Bota e majtë



Bota e djathtë



$\mathcal{A}$

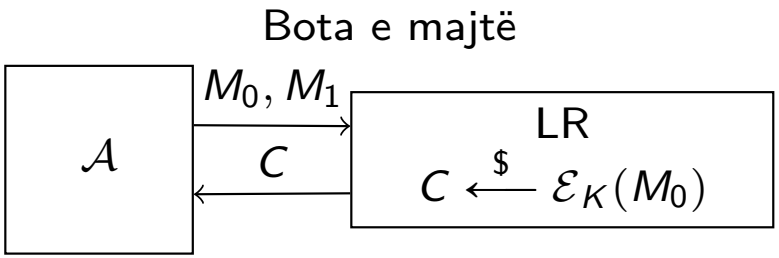
$C_1 \leftarrow \mathrm{LR}(0^n, 0^n)$

$C_2 \leftarrow \mathrm{LR}(0^n, 1^n)$

$d \xleftarrow{\$} \mathcal{B}(C_1, C_2)$

return d

XOR-pasiguria implikon IND-CPA-pasigurinë (Vazhdim)



$\mathcal{A}$

$C_1 \leftarrow \mathrm{LR}(0^n, 0^n)$

$C_2 \leftarrow \mathrm{LR}(0^n, 1^n)$

$d \xleftarrow{\$} \mathcal{B}(C_1, C_2)$

return d

- Çfarë ndodh:
  - $C_1 \xleftarrow{\$} \mathcal{E}_K(0^n)$ dhe $C_2 \xleftarrow{\$} \mathcal{E}_K(0^n)$
  - XOR i bitëve të fundit të mesazheve është 0
  - Kështu që $\mathcal{B}$ kthen 0
- Prandaj,

$$\Pr[\mathrm{Left}^{\mathcal{A}}_{\mathcal{SE}} = 1] = 0.$$

XOR-pasiguria implikon IND-CPA-pasigurinë (Vazhdim)

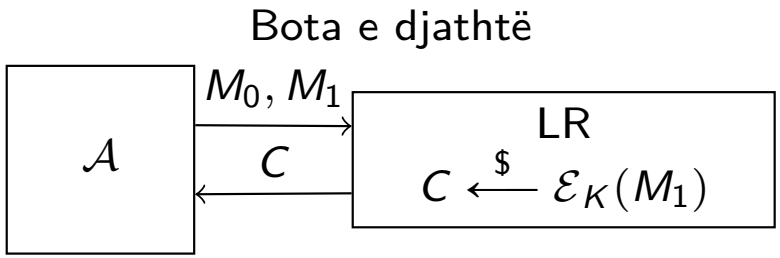
$\mathcal{A}$

$C_1 \leftarrow \mathrm{LR}(0^n, 0^n)$

$C_2 \leftarrow \mathrm{LR}(0^n, 1^n)$

$d \xleftarrow{\$} \mathcal{B}(C_1, C_2)$

return d



- Çfarë ndodh:
  - $C_1 \xleftarrow{\$} \mathcal{E}_K(0^n)$ dhe $C_2 \xleftarrow{\$} \mathcal{E}_K(1^n)$
  - XOR i bitëve të fundit të mesazheve është 1
  - Kështu që $\mathcal{B}$ kthen 1
- Prandaj,

$$\Pr[\mathrm{Right}^{\mathcal{A}}_{\mathcal{SE}} = 1] = 1.$$

XOR-pasiguria implikon IND-CPA-pasigurinë (Vazhdim)

- Kështu,

$$\begin{aligned}\mathsf{Adv}^{\mathrm{ind-cpa}}_{\mathcal{SE}}(\mathcal{A}) &= \Pr[\mathsf{Right}^{\mathcal{A}}_{\mathcal{SE}} = 1] - \Pr[\mathsf{Left}^{\mathcal{A}}_{\mathcal{SE}} = 1] \\ &= 1 - 0 = 1,\end{aligned}$$

siç pohuam.

Siguria e CTRC

- Le të jetë $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ një blok shifrues. Dërguesi mban një numërues *ctr*, fillimisht 0. Skema është $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$, ku

$\mathcal{E}_K(M)$

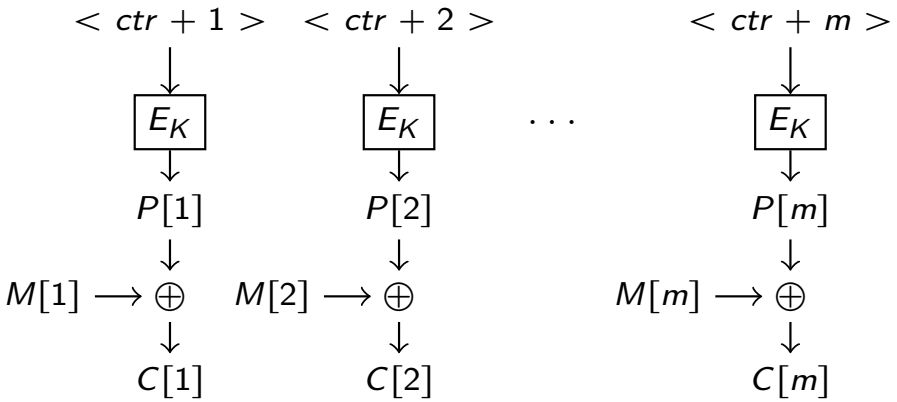
$C[0] \leftarrow ctr$

for $i = 1, \ldots, m$ **do**

$P[i] \leftarrow E_K(< ctr + i >)$

$C[i] \leftarrow P[i] \oplus M[i]$

return C



- Pyetje: A është $\mathcal{SE}$ IND-CPA i sigurt?
  - Një gjë e tillë nuk mund të pritet në qoftë se E është „i keq“. Prandaj të riformulojmë pyetjen:
- Pyetje: Në qoftë se E është „i mirë“ (PRF), atëherë a është $\mathcal{SE}$ IND-CPA i sigurt?
- Përgjegjja: Po.