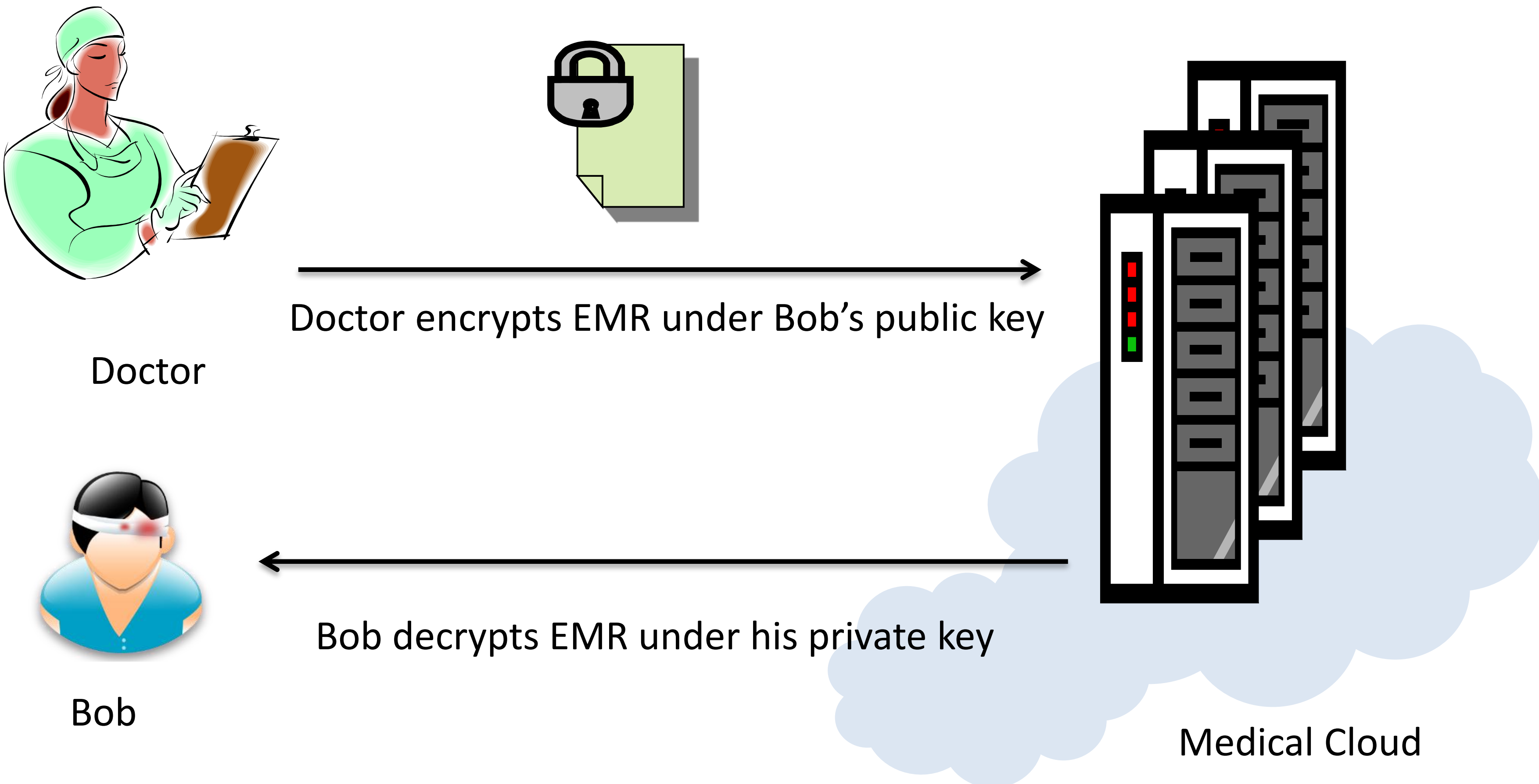
Attribute-Based Encryption

陳榮傑
交通大學資工系
Cryptanalysis Lab
6/25/2012

Public Key Encryption



Limitations

- Bob is the single and known recipient of data

  - Unknown recipient?
  - Many recipients?
  - More may join system later?

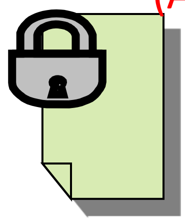
Attribute-Based Encryption [SW05]

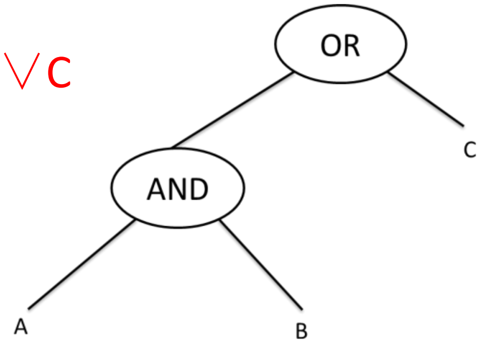
Flexible data sharing:

Idea

Ciphertexts: associated with access formulae

$(A \wedge B) \vee C$



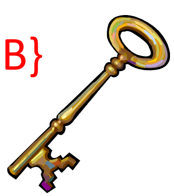


Private Keys: associated with attributes

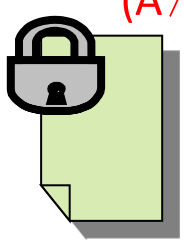
{A, B}

Decryption:

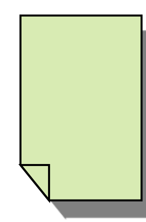
{A, B}



$(A \wedge B) \vee C$

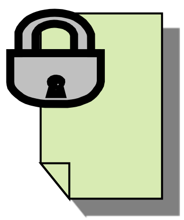


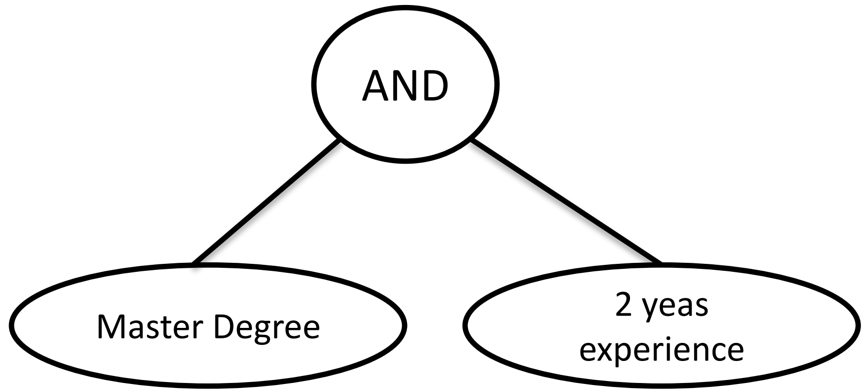
{A, B} satisfies $(A \wedge B) \vee C$



Example 1: Job Posting

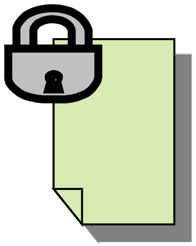
Encrypt a job posting

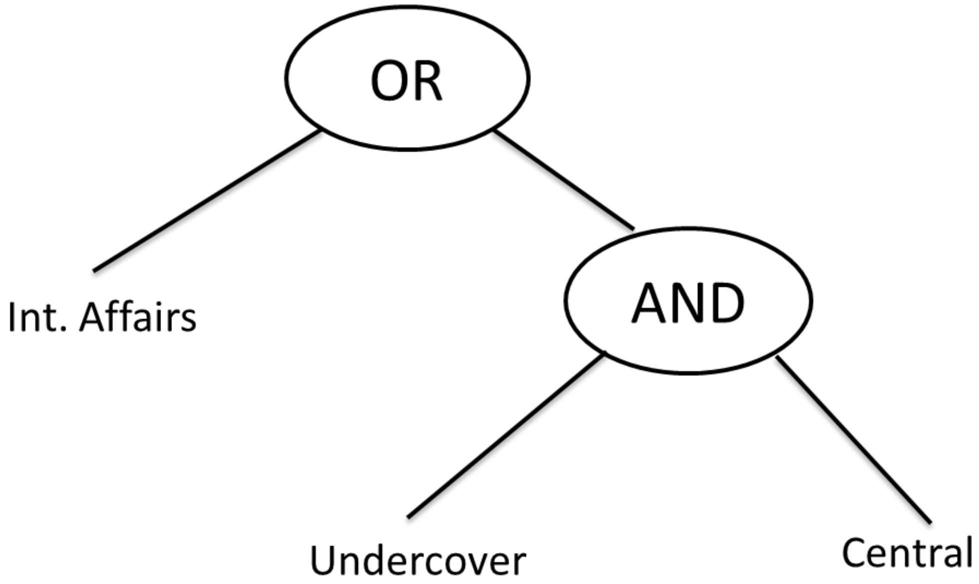




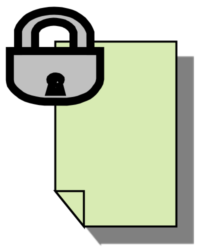
Example 2: Police Department

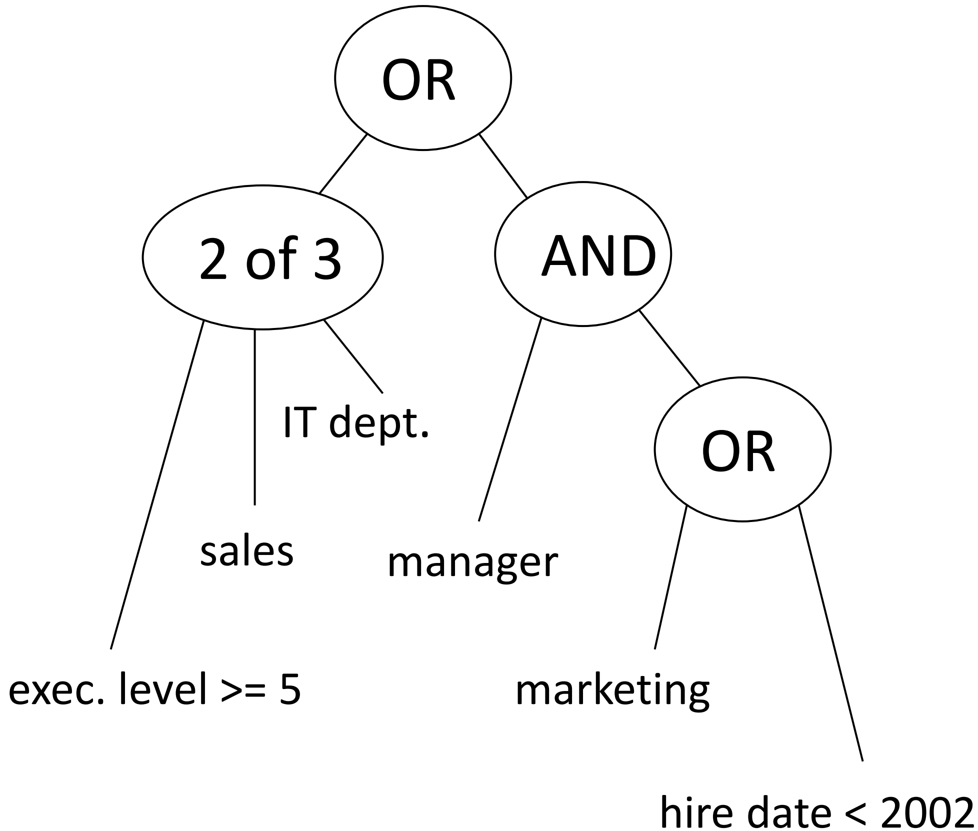
An informant encrypts a message for anyone in the internal affairs office or anyone who is undercover and in the central office .



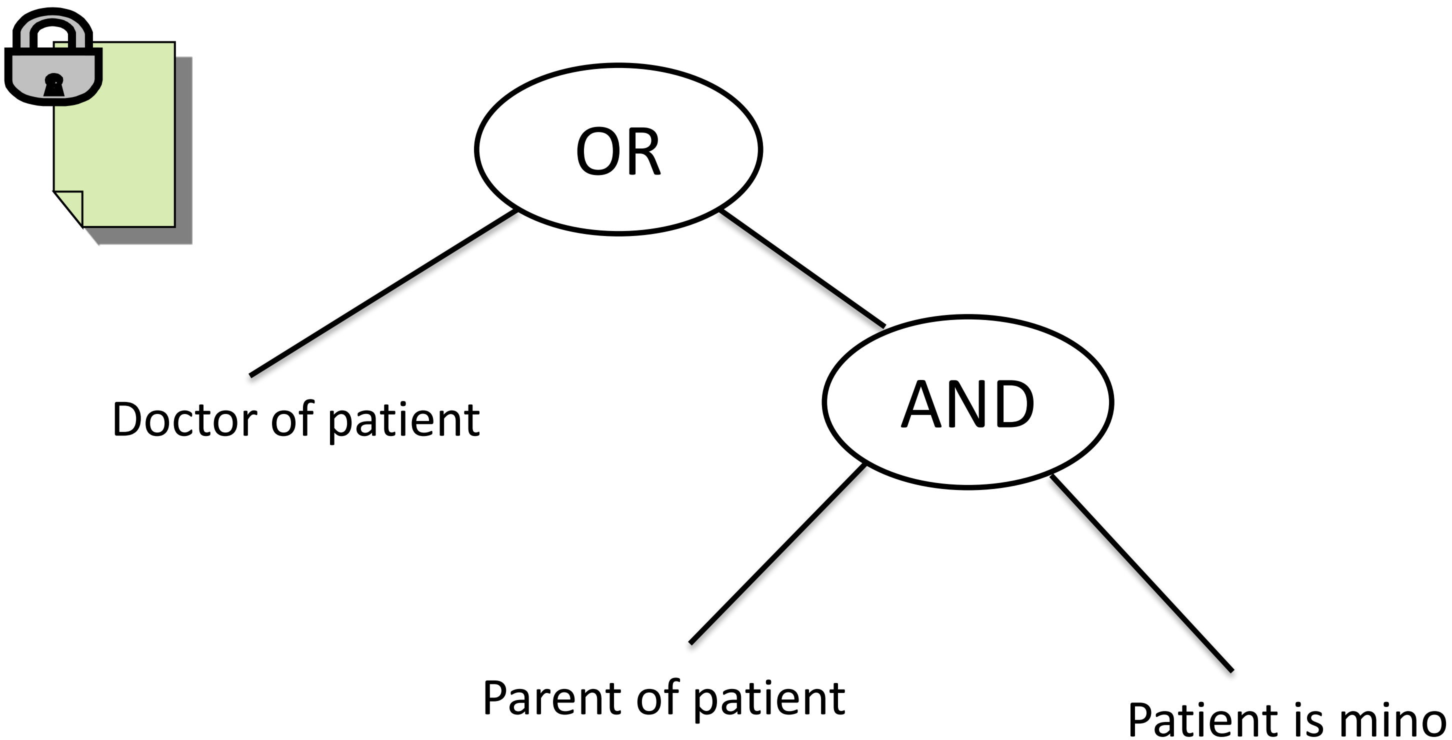


Example 3: Technology Company

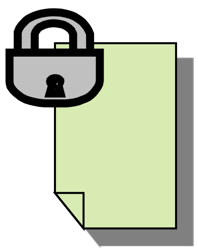


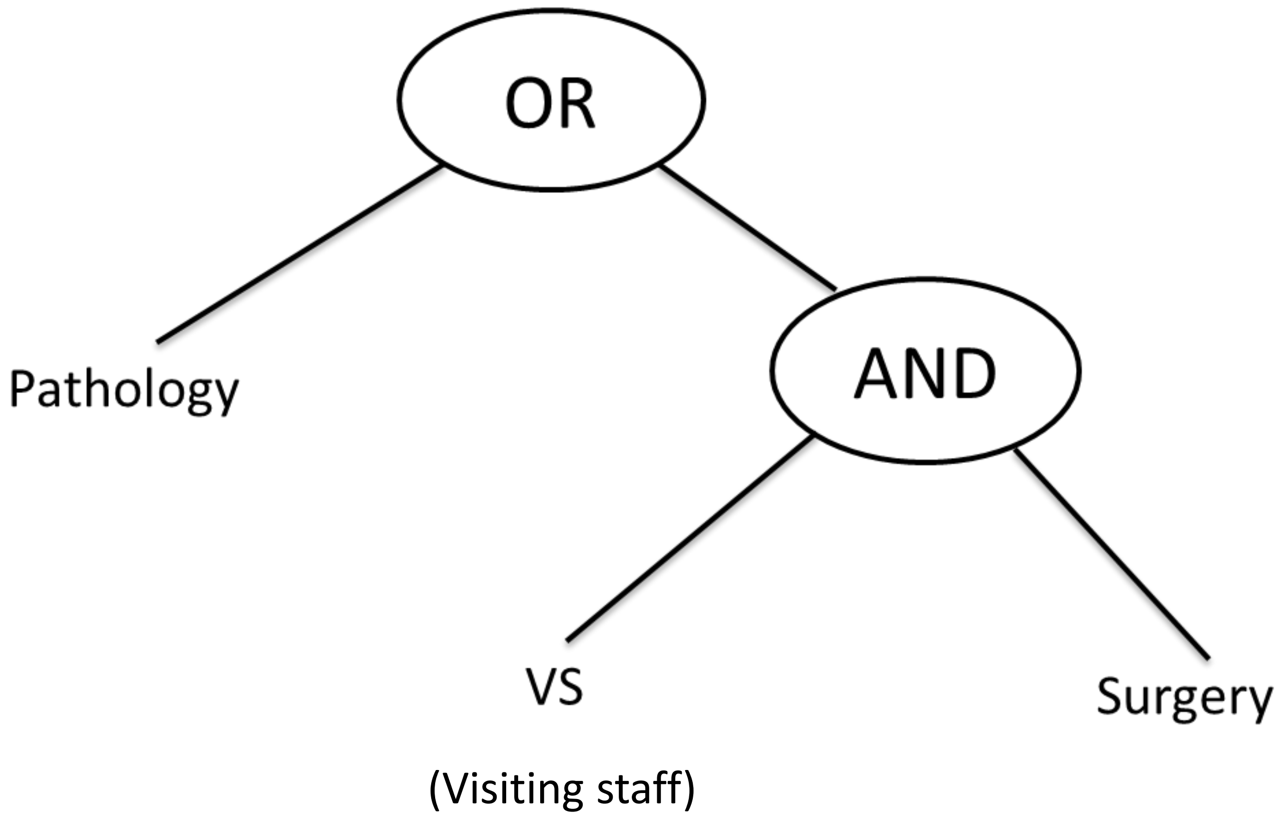


Example 4: Johns Hopkins Hospital

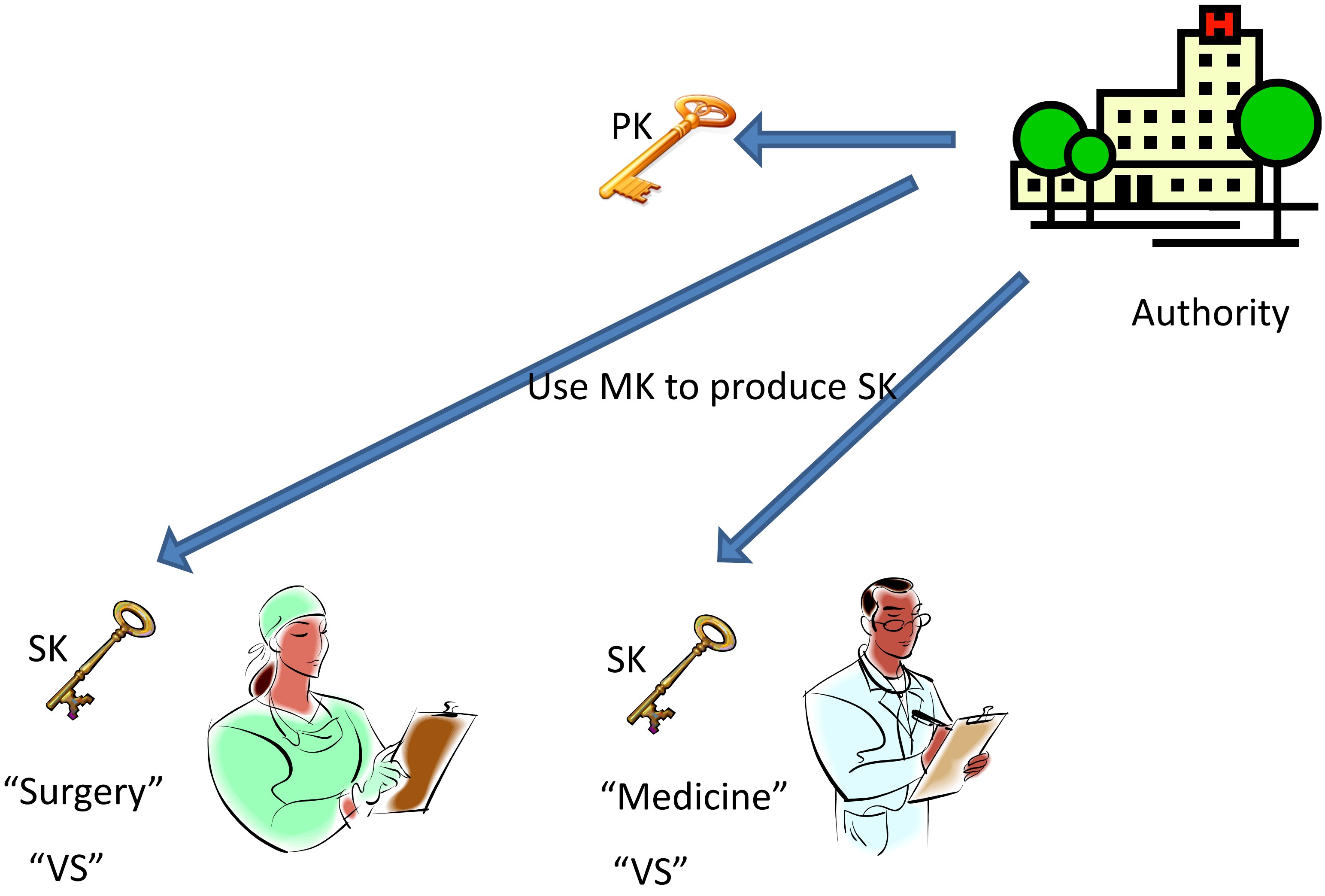


Example 5: EMR (Electronic medical record)

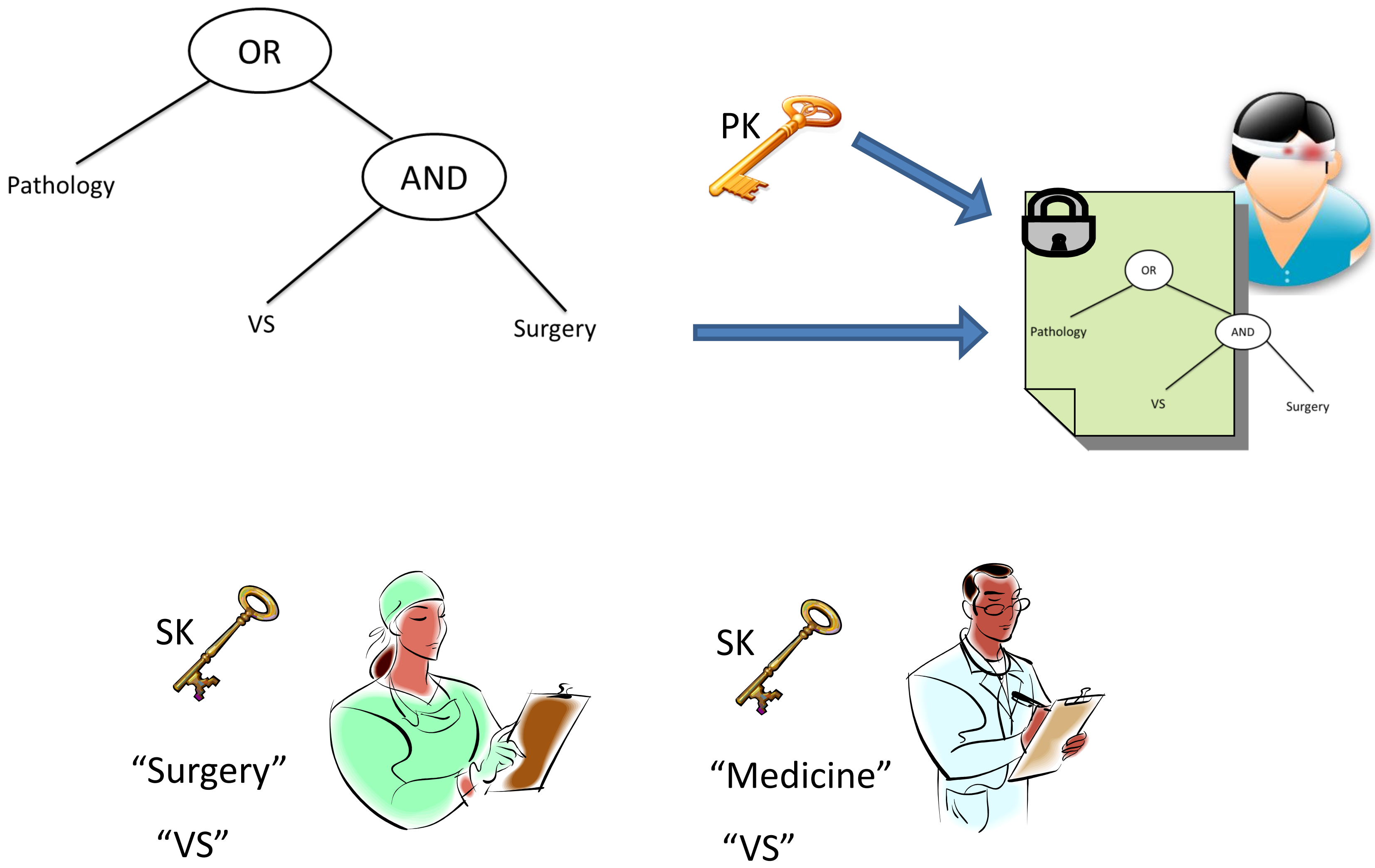




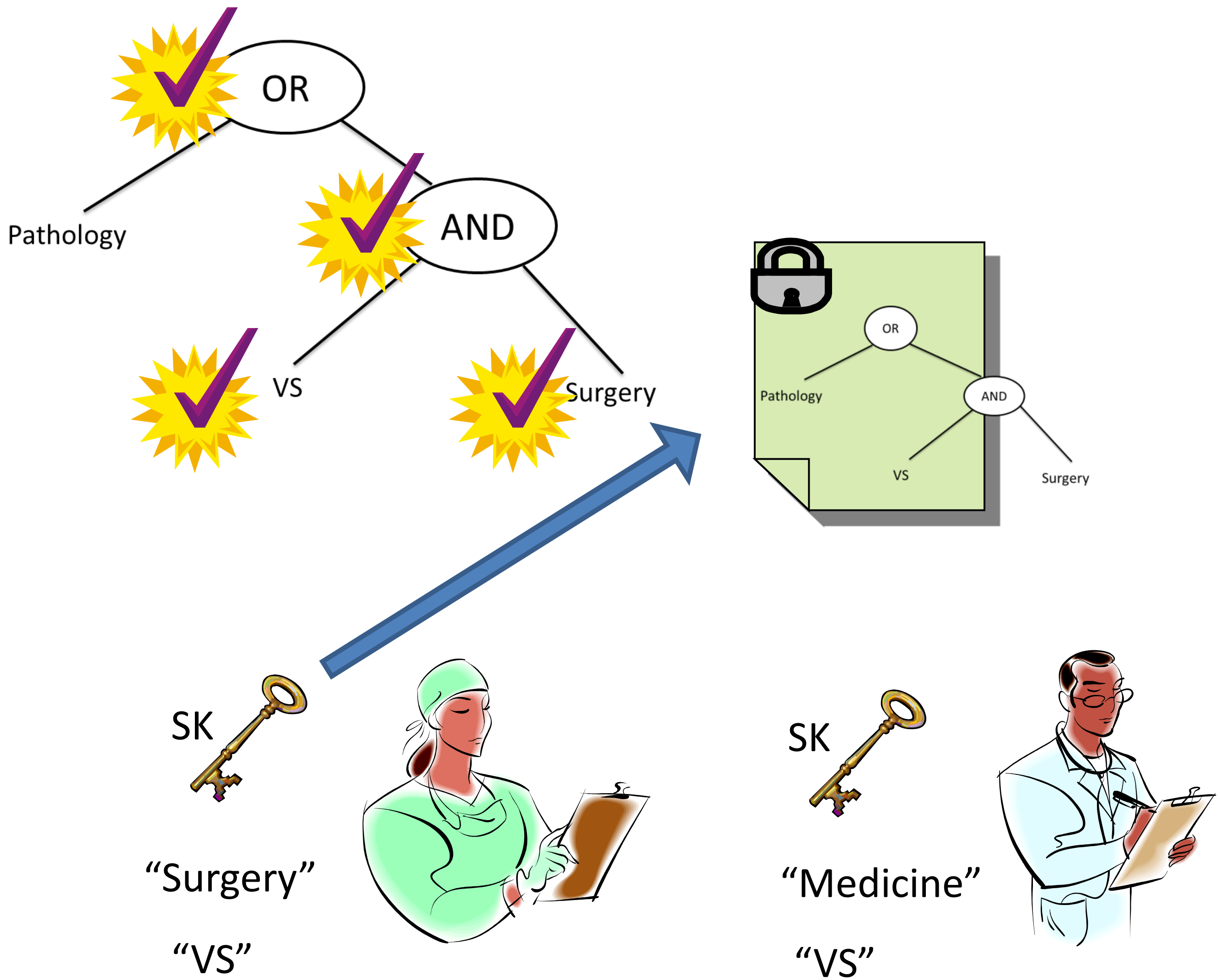
Example 5: EMR (Electronic medical record)



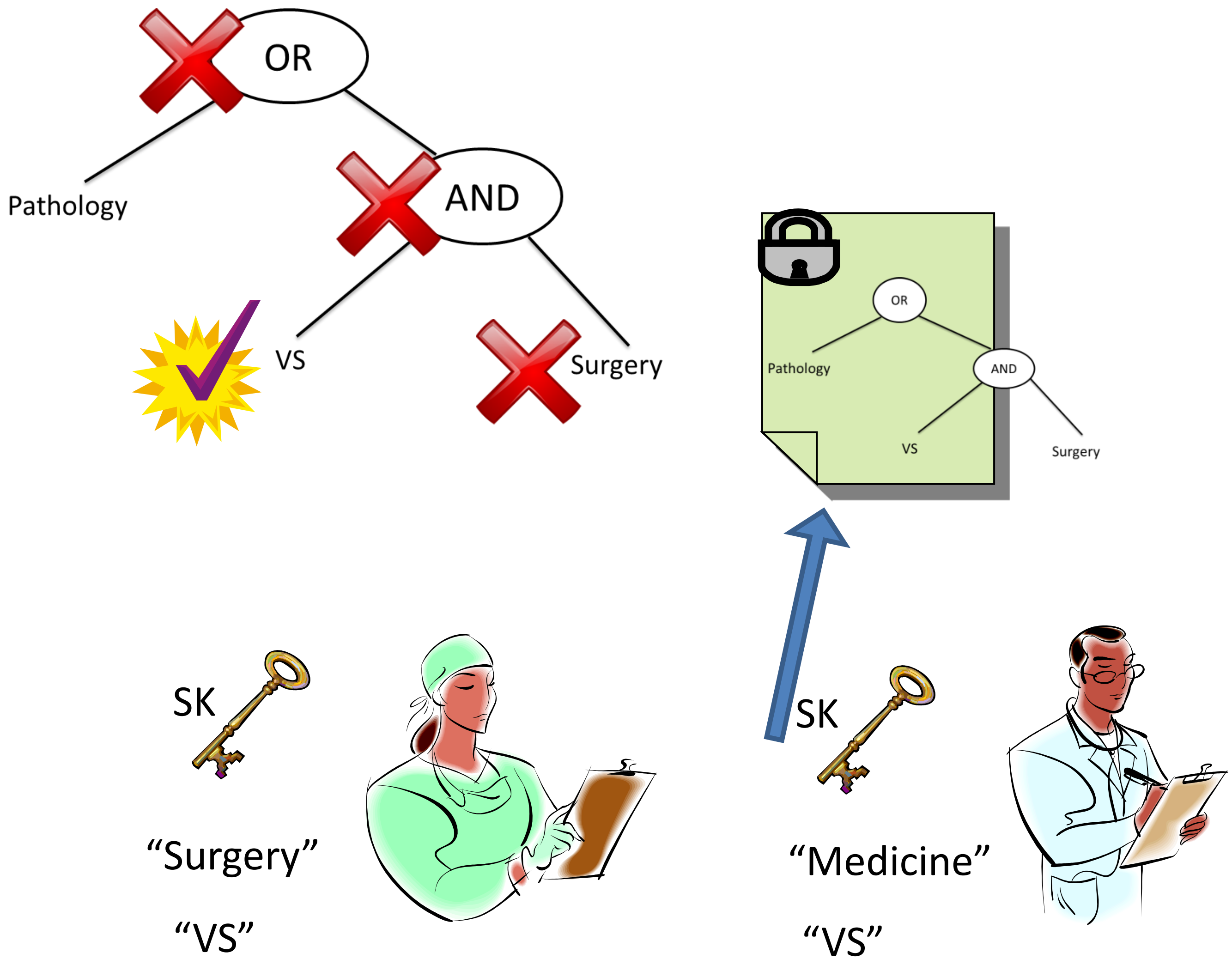
Example 5: EMR



Example 5: EMR

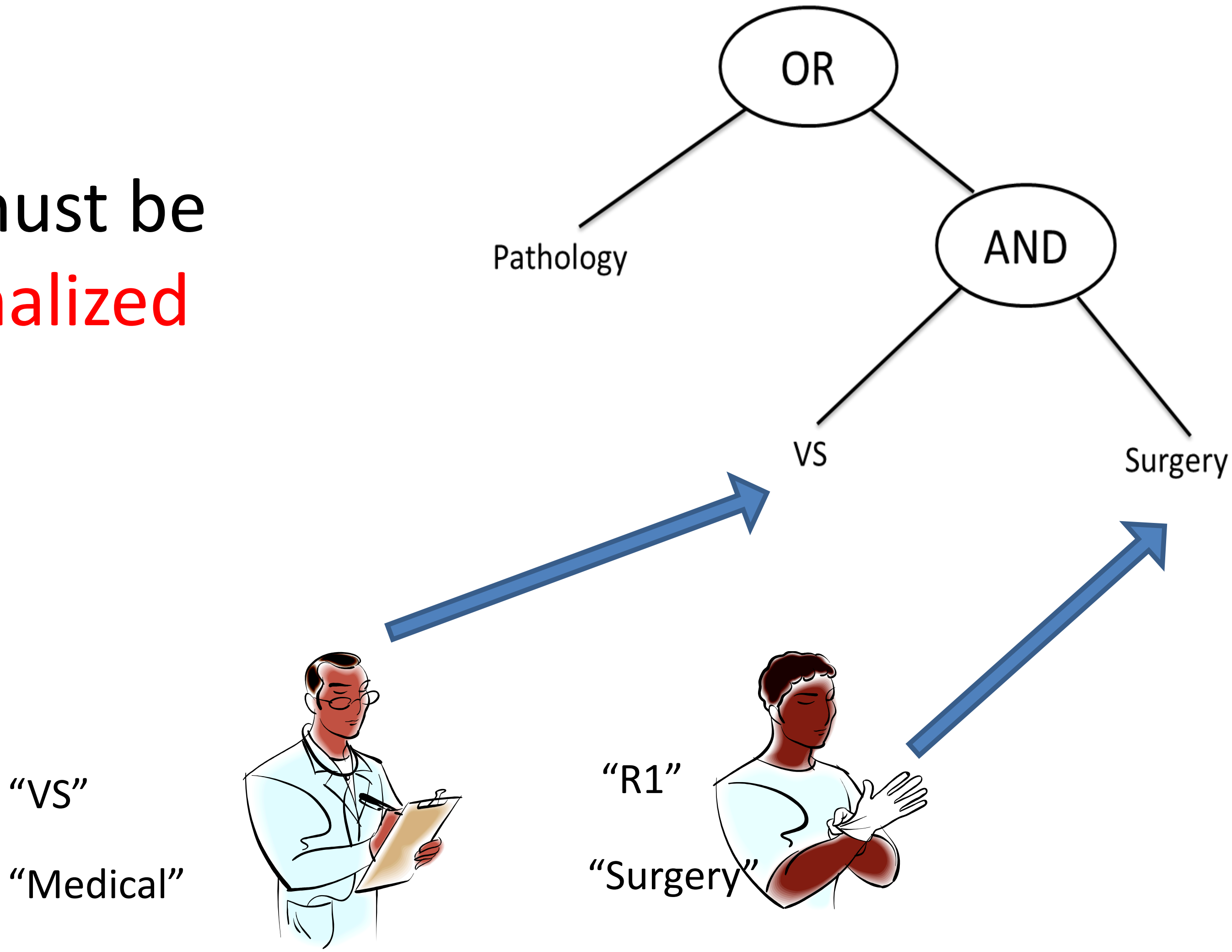


Example 5: EMR



Avoid Collusion Attacks

Keys must be personalized



Key Personalization

r’

VS

“VS”

Choose random r for each user’s all attributes

r’’

Surgery

So they can’t collude!

“Surgery”

[BSW07,LW11] CIPHER-POLICY ABE

Cipher-policy ABE

- Secret keys are labeled with a set of attributes
- Ciphertext is associated with access structure that control which user is able to decrypt the ciphertext.

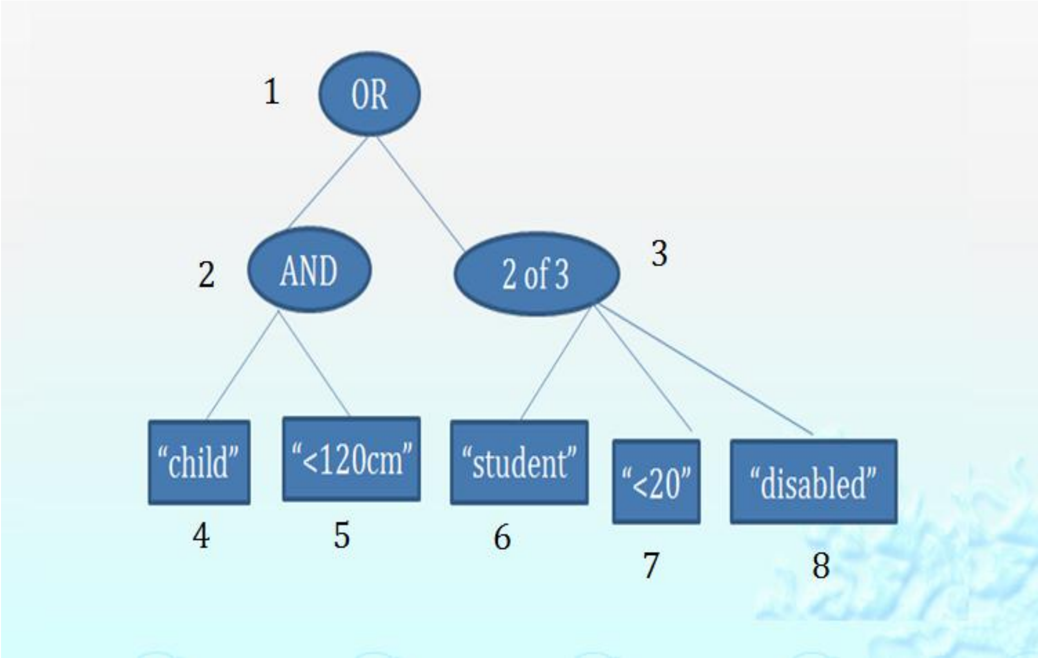
Setup

- Bilinear map: e
  - e: $G_1 \times G_1$ -> G_2
  - G_1 has prime order p
  - g is a generator of G_1

Setup

- U = {a_1=child, a_2=<120cm, … ,a_n }
  - U is the set of all attributes

- H: U -> G_1



Setup

- MK(master key): used to produce user's secret key
  - Choose $\alpha, \beta \in Z_p$
  - MK = (β, g^{α})

- PK(public key): used to produce ciphertext
  - PK=$(g, g^{\beta}, e(g, g)^{\alpha})$

Encryption

- Encrypt(M(plaintext), T(access tree), PK)

  Choose a polynomial q_x for each node: $q_1, q_2, q_3, \dots, q_8$.

  degree(q_x) = K(x) - 1
  degree(q_1) = 0
  degree(q_2) = 1
  degree(q_3) = 1
  degree(q_4) = 0
  degree(q_8) = 0

- Encrypt(M(plaintext), T(access tree), PK)

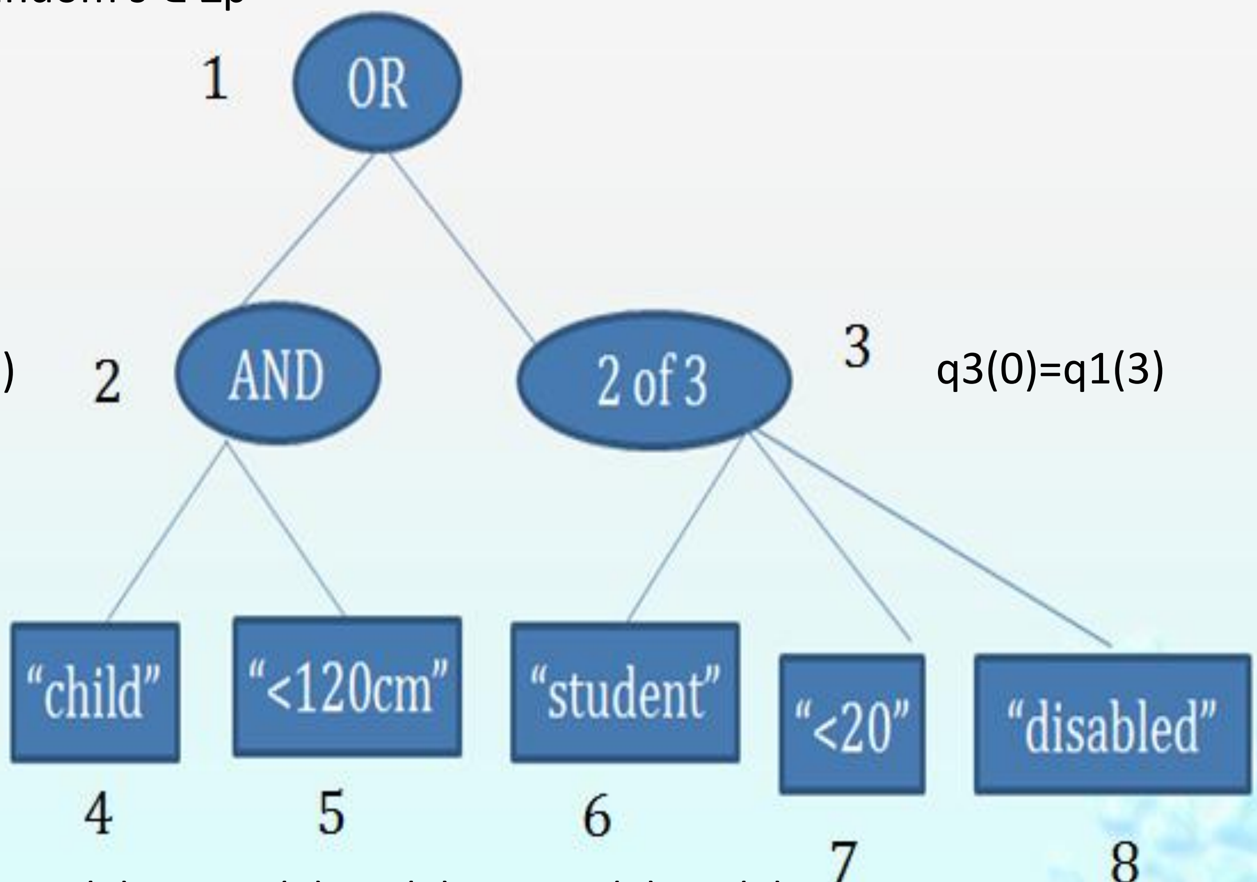
  Choose a polynomial q_x for each node: $q_1, q_2, q_3, \dots, q_8$.

  degree(q_x) = K(x) - 1
  degree(q_1) = 0
  degree(q_2) = 1
  degree(q_3) = 1
  degree(q_4) = 0
  degree(q_8) = 0

Encryption

Choose a random $s \in Z_p$

$q_1(0)=s$



q2(0)=q1(2)

q3(0)=q1(3)

q4(0)=q2(4)

q5(0)=q2(5)

q6(0)=q3(6)

q8(0)=q3(8)

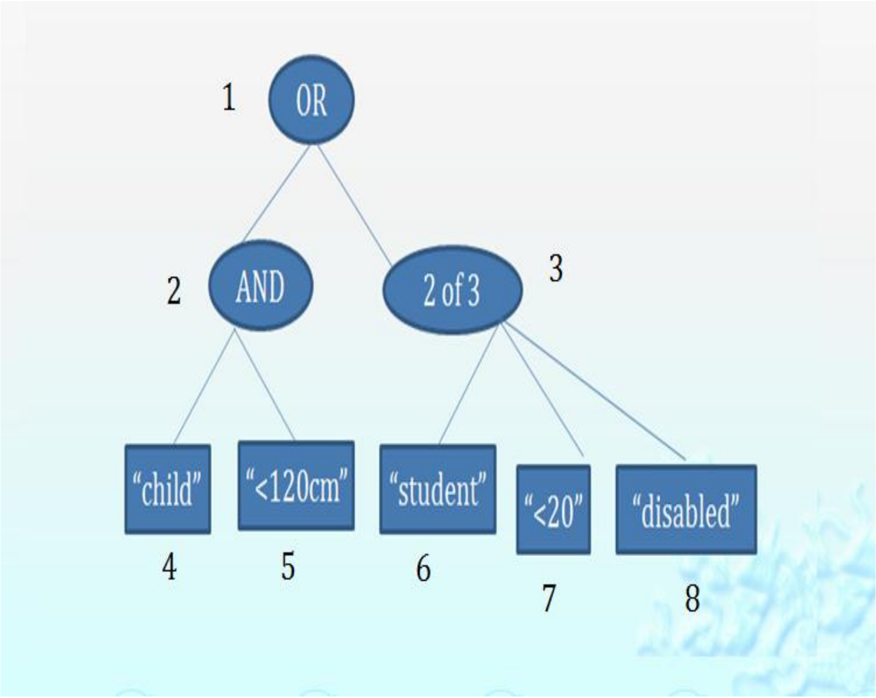
q7(0)=q3(7)

Encryption

- Output
  - T, $Me(g, g)^{\alpha s}$, $C=g^{\beta s}$
  - $C4 = g^{q_4(0)}$

    C8
  - $C4' = H(child)^{q_4(0)}$

    C8'



Key Generation

- KeyGen(γ = { “child”, “student”, “<20” }, MK)
  - Choose r $\in Z_p$
  - Choose $r_{child}, r_{student}, r_{<20}$ $\in Z_p$
  - Output
    - D = $g^{(\alpha+r)/\beta}$
    - $D_{child} = g^{r} \times H(\text{child})^{r_{child}}$

      $D_{student}$

      $D_{<20}$

    - $D'_{child} = g^{r_{child}}$

      $D'_{student}$

      $D'_{<20}$

Decryption

- Cipher text C
  - T, $Me(g,g)^{\alpha s}$, C = $g^{\beta s}$
  - $C4 = g^{q_4(0)}$

    C8
  - $C4' = H(child)^{q_4(0)}$

    C8'

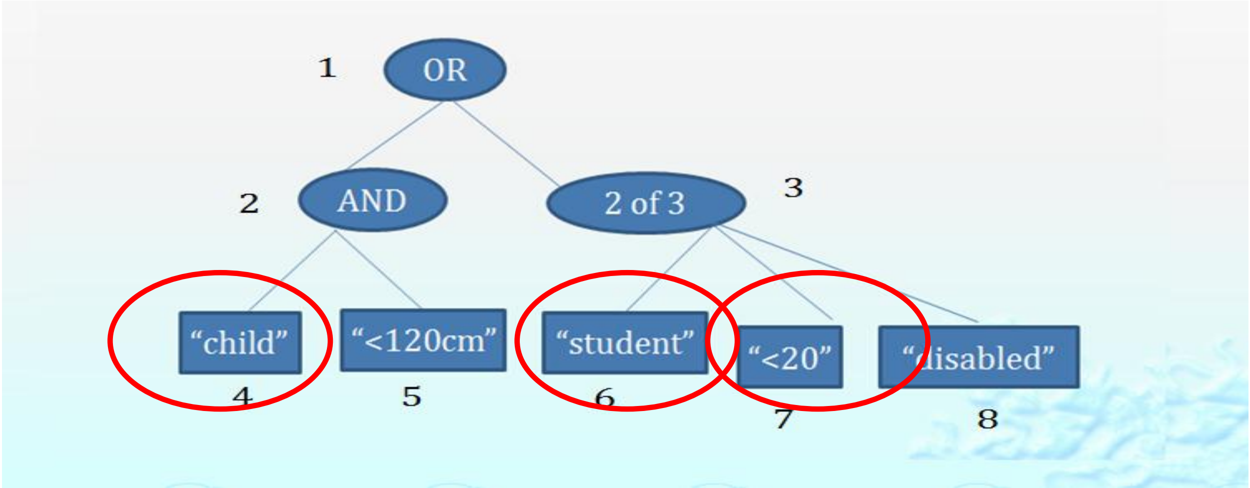
- Private Key
  - $D = g^{(\alpha+r)/\beta}$
  - $D_{child} = g^{r} \times H(\text{child})^{r_{child}}$

    $D_{student}$

    $D_{<20}$
  - $D'_{child} = g^{r_{child}}$

    $D'_{student}$

    $D'_{<20}$



- $\frac{e(D_{student}, C_6)}{e(D'_{student}, C'_6)} = e(g, g)^{r q_6(0)}$

$$= \frac{e(D_i, C_x)}{e(D'_i, C'_x)}$$
$$= \frac{e\left(g^r \cdot H(i)^{r_i}, h^{q_x(0)}\right)}{e(g^{r_i}, H(i)^{q_x(0)})}$$
$$= e(g, g)^{r q_x(0)}.$$

- $e(g, g)^{r q_1(0)} = e(g, g)^{rs}$

$$\mathrm{Me}(g,g)^{\alpha s} \;/\; e(C, D)$$

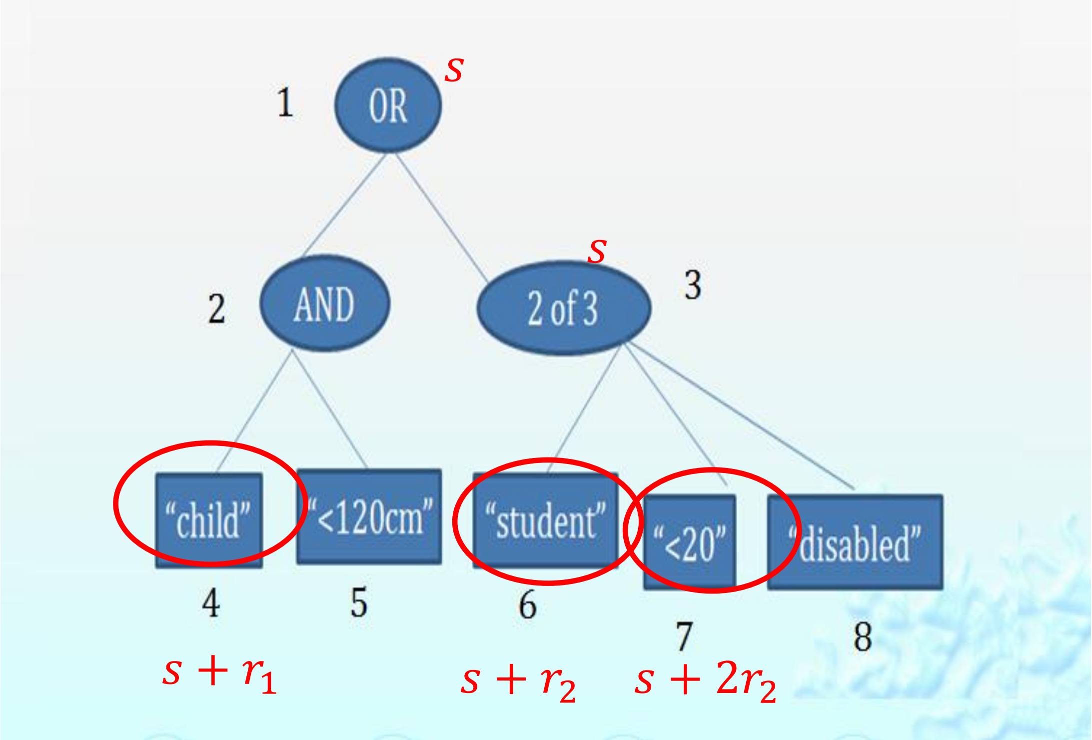
$$= \mathrm{Me}(g,g)^{\alpha s} \;/\; e(g^{\beta s}, g^{(\alpha+r)/\beta})$$

$$= \mathrm{Me}(g,g)^{-rs}$$

$$\mathrm{Me}(g,g)^{-rs} \cdot e(g,g)^{rs} = \mathrm{M}$$

Our implementation
(Linear Secret Sharing Scheme)

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & -1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 2 \\ 1 & 0 & 3 \end{pmatrix} \cdot \begin{pmatrix} s \\ r_1 \\ r_2 \end{pmatrix} = \begin{pmatrix} s + r_1 \\ -r_1 \\ s + r_2 \\ s + 2r_2 \\ s + 3r_2 \end{pmatrix} \begin{array}{l} \text{(for 4)} \\ \text{(for 5)} \\ \text{(for 6)} \\ \text{(for 7)} \\ \text{(for 8)} \end{array}$$



病歷首頁單

病患姓名：	Bob	**身分證字號：**	A123456789	**病歷號碼：**	123456	**性別：**	男	**文件產生時間：**	2009-11-25 04:00:00
婚姻狀況：	已婚	**出生地：**	台灣台北市	**生日：**	2000-01-01	**地址：**	台北縣三峽鎮大智路100號10樓之10		

家用電話(H)：(02) 12345678	公司電話(O)：(02) 12345678	手機：921111998	mailto:22223333@gmail.com

配偶姓名：配偶姓名

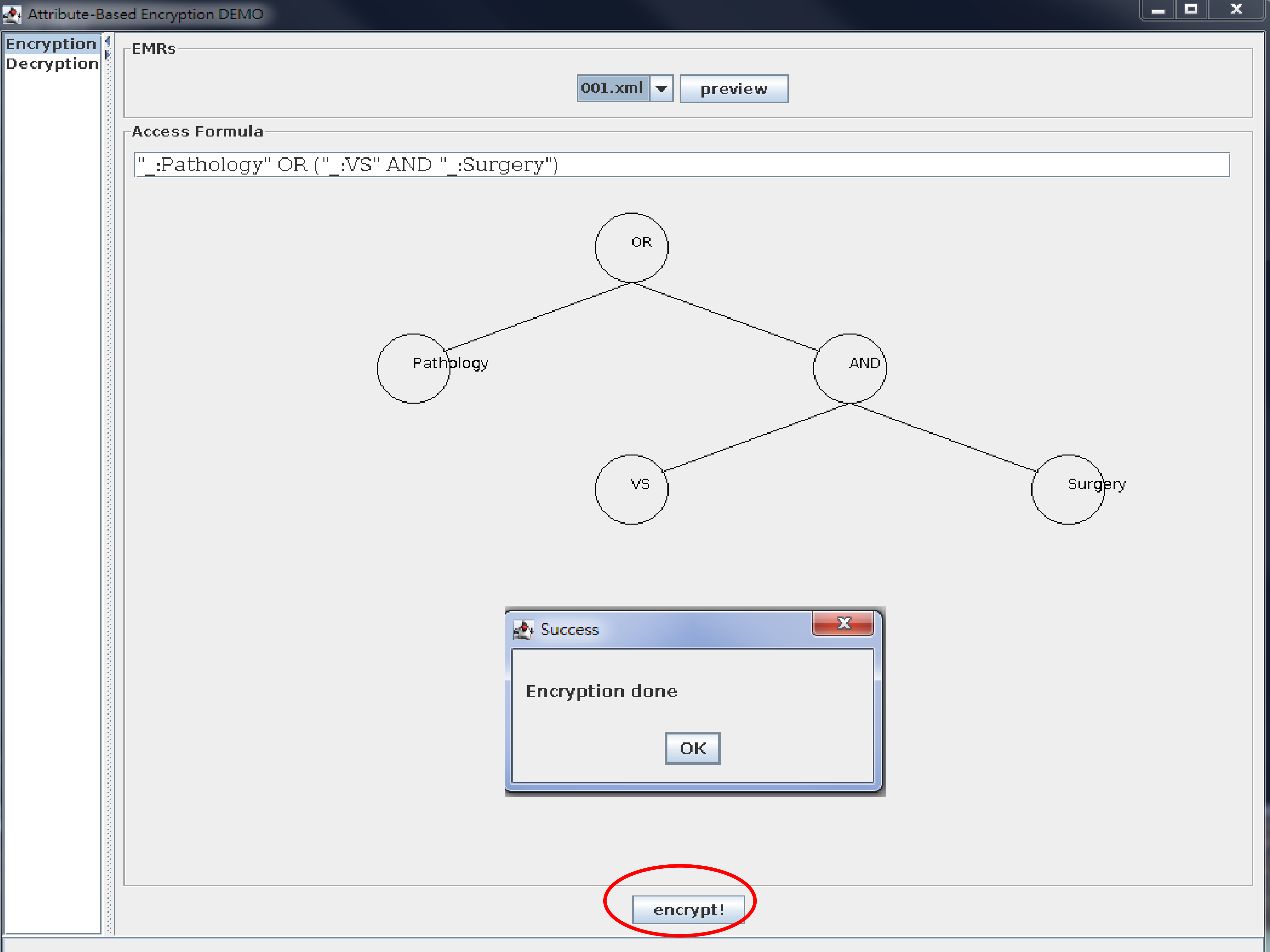
緊急連絡人：張爸	**關係：**	**家用電話(H)：**(02) 12345678	**公司電話(O)：**(02) 12345678	**手機：**921111998	mailto:22223333@gmail.com
緊急連絡人：張媽	**關係：**	**家用電話(H)：**(02) 12345678	**公司電話(O)：**(02) 12345678	**手機：**921111998	mailto:22223333@gmail.com

登錄者：	范醫師	**單位：**	外科部	**醫院代碼：**	H0001	**卡號：**	H23456	**證號：**	H12345	**簽屬時間：**	2001-01-01
最後簽核者：		**簽屬時間：**	--								

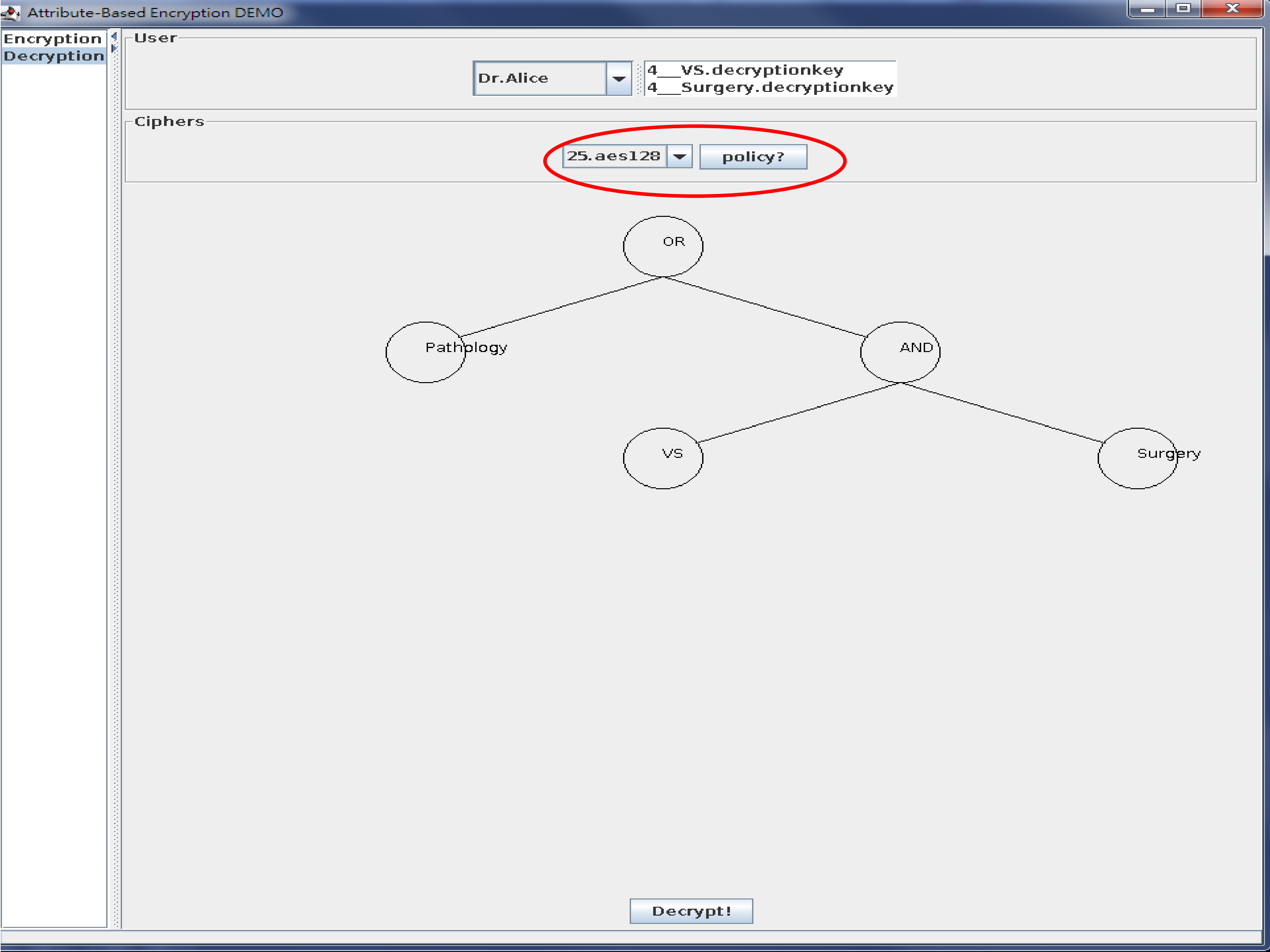
各類過去病史

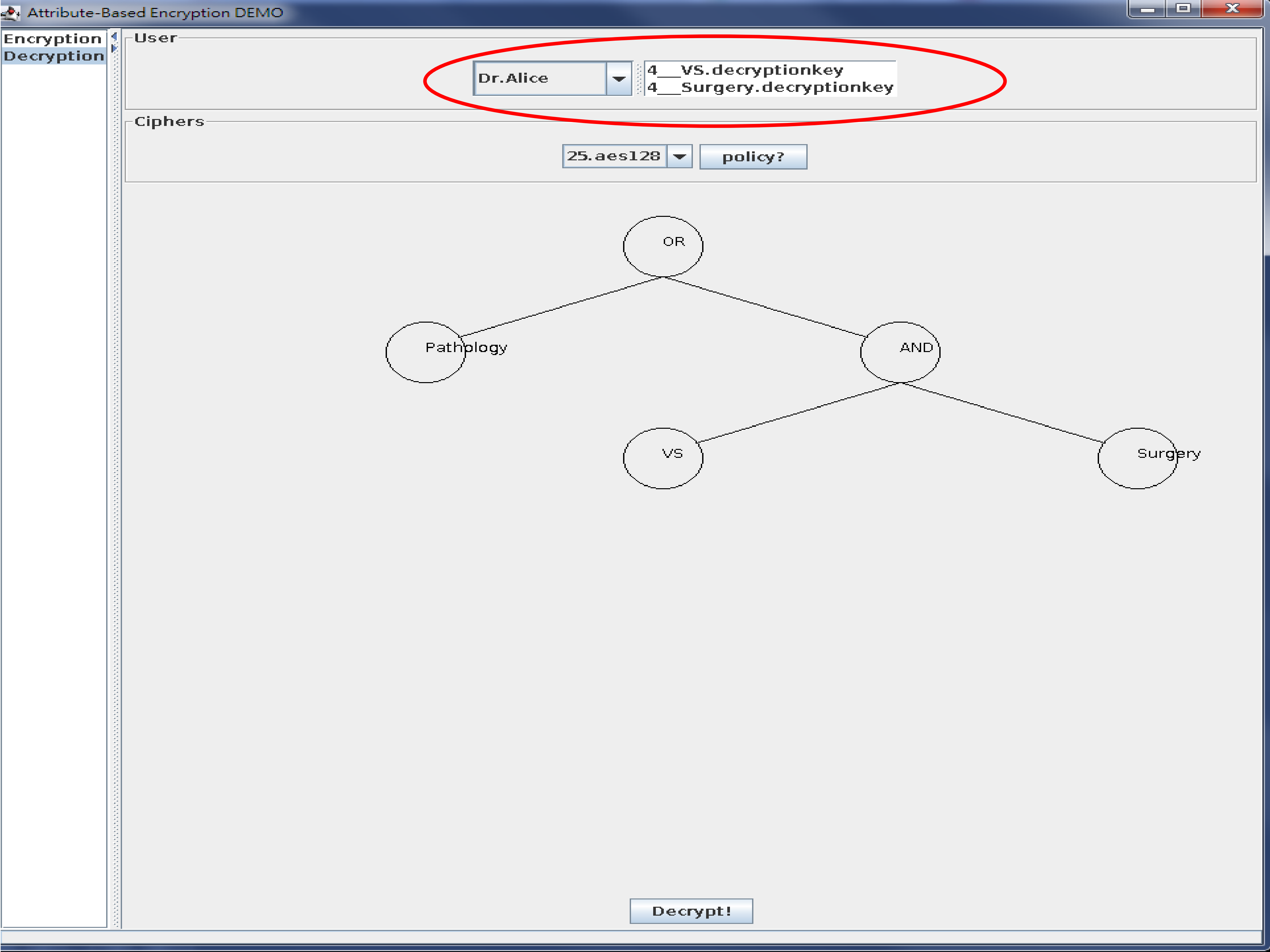
- 重大傷病：(文字敘述)
- 過敏史-藥物過敏：(文字敘述)
- 過敏史-食物過敏：(文字敘述)
- 過敏史-環境過敏：(文字敘述)
- 藥物不良反應(ADR)：(文字敘述)
- 旅遊史：(文字敘述)
- 傳染病史：(文字敘述)
- 遺傳病史：(文字敘述)

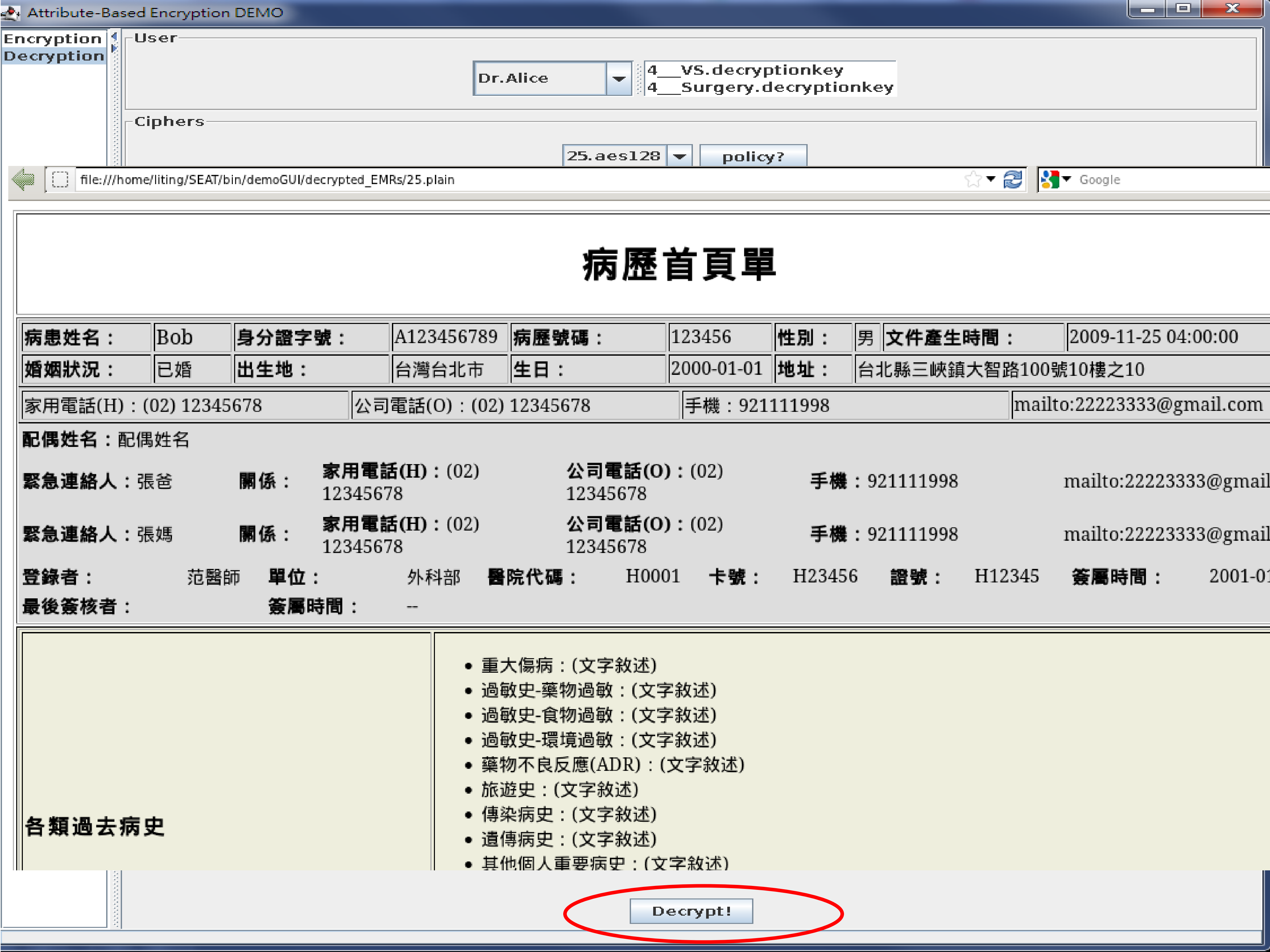
Continuity of Care Document:
XML-based standard

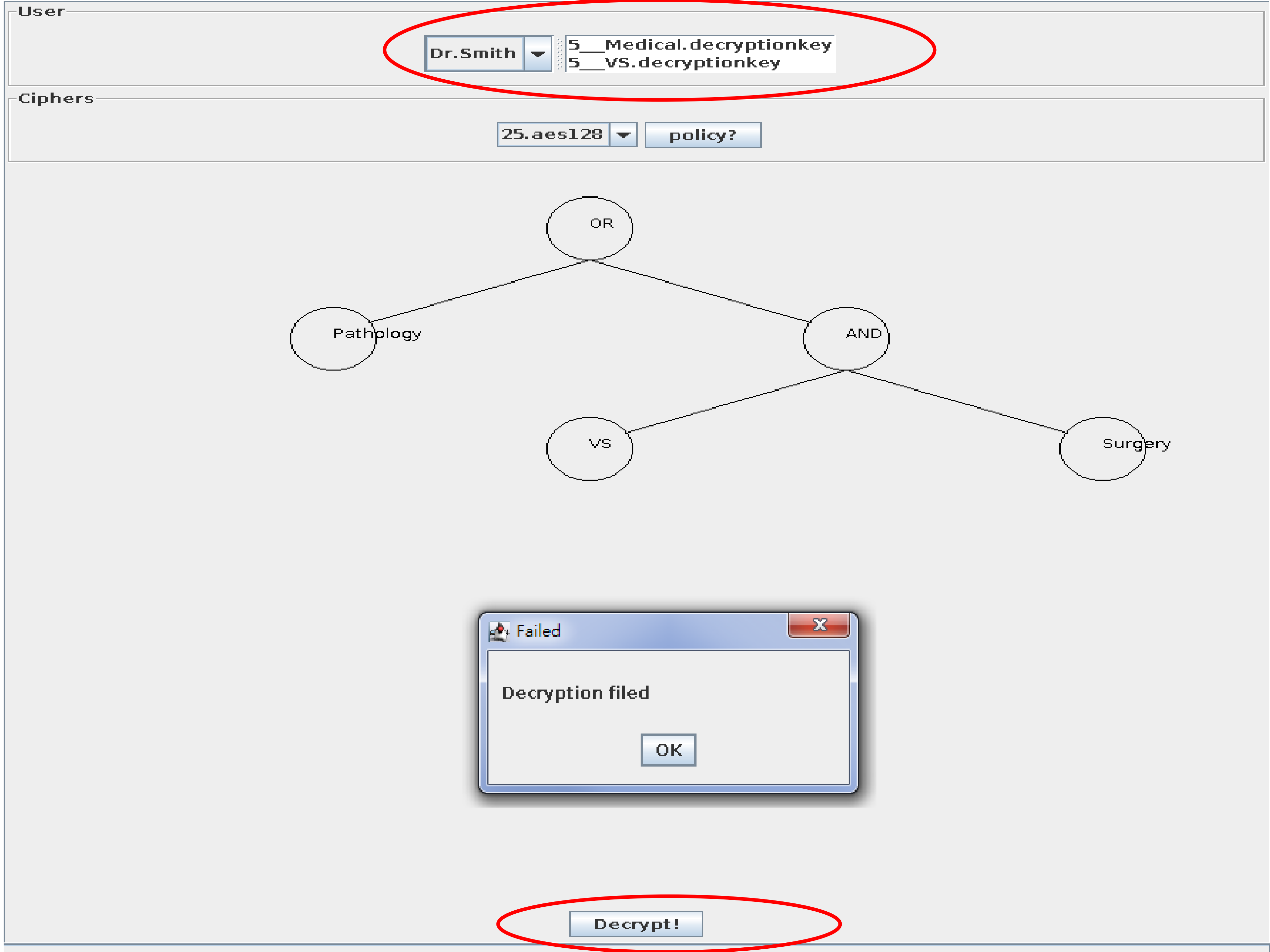


Attribute-Based Encryption DEMO
Encryption
Decryption
EMRs
001.xml
preview
Access Formula
"_:Pathology" OR ("_:VS" AND "_:Surgery")
OR
Pathology
AND
VS
Surgery
Success
Encryption done
OK
encrypt!


Attribute-Based Encryption DEMO
Encryption
Decryption
User
Dr.Alice
4__VS.decryptionkey
4__Surgery.decryptionkey
Ciphers
25.aes128
policy?
OR
Pathology
AND
VS
Surgery
Decrypt!


Attribute-Based Encryption DEMO
Encryption
Decryption
User
Dr.Alice
4__VS.decryptionkey
4__Surgery.decryptionkey
Ciphers
25.aes128
policy?
OR
Pathology
AND
VS
Surgery
Decrypt!


Attribute-Based Encryption DEMO
Encryption
Decryption
User
Dr.Alice
4__VS.decryptionkey
4__Surgery.decryptionkey
Ciphers
25.aes128
policy?
file:///home/liting/SEAT/bin/demoGUI/decrypted_EMRs/25.plain
Google
病歷首頁單
病患姓名： Bob 身分證字號： A123456789 病歷號碼： 123456 性別： 男 文件產生時間： 2009-11-25 04:00:00
婚姻狀況： 已婚 出生地： 台灣台北市 生日： 2000-01-01 地址： 台北縣三峽鎮大智路100號10樓之10
家用電話(H)：(02) 12345678 公司電話(O)：(02) 12345678 手機：921111998 mailto:22223333@gmail.com
配偶姓名：配偶姓名
緊急連絡人：張爸 關係： 家用電話(H)：(02) 12345678 公司電話(O)：(02) 12345678 手機：921111998 mailto:22223333@gmail
緊急連絡人：張媽 關係： 家用電話(H)：(02) 12345678 公司電話(O)：(02) 12345678 手機：921111998 mailto:22223333@gmail
登錄者： 范醫師 單位： 外科部 醫院代碼： H0001 卡號： H23456 證號： H12345 簽屬時間： 2001-0
最後簽核者： 簽屬時間： --
各類過去病史
重大傷病：(文字敘述)
過敏史-藥物過敏：(文字敘述)
過敏史-食物過敏：(文字敘述)
過敏史-環境過敏：(文字敘述)
藥物不良反應(ADR)：(文字敘述)
旅遊史：(文字敘述)
傳染病史：(文字敘述)
遺傳病史：(文字敘述)
其他個人重要病史：(文字敘述)
Decrypt!


User
Dr.Smith
5__Medical.decryptionkey
5__VS.decryptionkey
Ciphers
25.aes128
policy?
OR
Pathology
AND
VS
Surgery
Failed
Decryption filed
OK
Decrypt!

- Questions?

- Thank you