ECE 471/571 Security Notions

perfect secrecy

$\forall$ r.v. X, $\forall x \in \mathcal{P}$ $y \in C$

$$P(X = x) = P(X = x \mid E_k(X) = y)$$

prior — posterior

plaintext and ciphertext are independent.... information-theoretically. $I(X; Y) = 0$

Given $Pr(X = x)$

$K \in \mathcal{K}$. random. $Pr(K = k)$

Y — ciphertext.

$$Pr(X = x \mid Y = y) = \frac{Pr(X = x, Y = y)}{Pr(Y = y)}$$

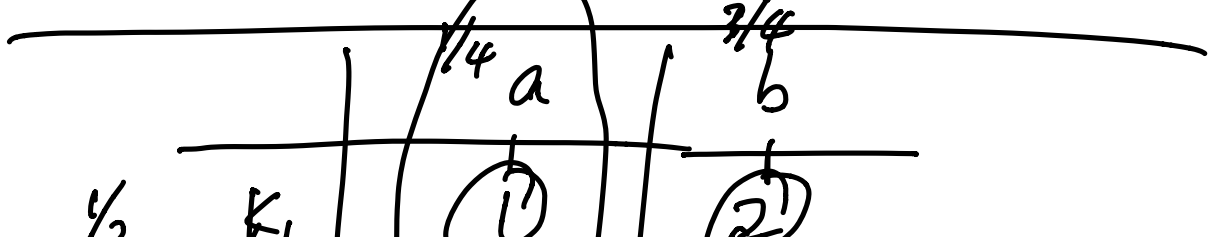
$$= \frac{Pr(Y = y \mid X = x) \cdot Pr(X = x)}{Pr(Y = y)}$$

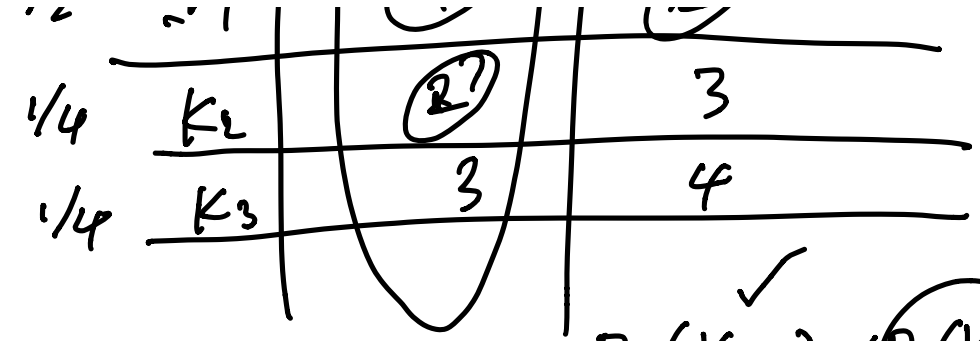
$Pr(X = x)$: prior

b.

$$Pr(Y = y) = \sum_{\{k:\, y \in C(k)\}} Pr(K = k)\, Pr(X = D_k(y))$$

$C(k)$: set of possible ciphers if k is key.





e.g. $Pr(X=a \mid Y=1) = \dfrac{Pr(X=a) \times Pr(Y=1 \mid X=a)}{Pr(Y=1)}$

$Pr(Y=1) = Pr(X=a) \cdot Pr(K=k_1)$

$= 1/4 \times 1/2 = \frac{1}{8}$

$Pr(Y=2) = 3/4 \times \frac{1}{2} + \frac{1}{4} \times \frac{1}{4} = \frac{7}{16}$

$Pr(Y=3) = \frac{1}{4} \times \frac{3}{4} + \frac{1}{4} \times \frac{1}{4} = \frac{1}{4}$

$Pr(Y=4) = \frac{1}{4} + 3/4 = 3/16$

$Pr(Y=1 \mid X=a) = Pr(K=k_1) = \frac{1}{2}.$

$= \dfrac{1/4 \times 1/2}{1/8} = 1$

$Pr(X=a) = 1/4. \neq 1$

NOT perfectly secret!

$$Pr(X=b \mid Y=1) = 0 \neq Pr(X=b)$$

$$Pr(X=a \mid Y=2) = \frac{1}{7}$$

$$Pr(X=b \mid Y=2) = \frac{6}{7}$$

One-time pad.

$n=2$.

k \ x	00	01	10	11
1/4 · 00	00	01	10	11
1/4 · 01	01	00	11	10
1/4 · 10	10	11	00	01
1/4 · 11	11	10	01	00