دانشکده‌ی علوم ریاضی

مقدمه‌ای بر رمزنگاری

پاسخ نامه سری ۱

نگارنده : آرش عاشوری

Problem 1

a) For the first implication, assume that E is perfectly Shannon secure. Consider any fixed $m \in M$ and $c \in C$.

$\Pr[\mathbf{c} = c \wedge \mathbf{m} = m] = \Pr[E(\mathbf{k}, \mathbf{m}) = c \wedge \mathbf{m} = m] = \Pr[E(\mathbf{k}, m) = c \wedge \mathbf{m} = m]$

$= \Pr[E(\mathbf{k}, m) = c] \Pr[\mathbf{m} = m]$ (by independence of k and m)

$$\begin{aligned}
\Pr[\mathbf{c} = c] &= \Pr[E(\mathbf{k}, \mathbf{m}) = c] \\
&= \textstyle\sum_{m' \in M} \Pr[E(\mathbf{k}, \mathbf{m}) = c \wedge \mathbf{m} = m'] && \text{(by total probability)} \\
&= \textstyle\sum_{m' \in M} \Pr[E(\mathbf{k}, m') = c \wedge \mathbf{m} = m'] \\
&= \textstyle\sum_{m' \in M} \Pr[E(\mathbf{k}, m') = c] \Pr[\mathbf{m} = m'] && \text{(by independence of k and m)} \\
&= \textstyle\sum_{m' \in M} \Pr[E(\mathbf{k}, m) = c] \Pr[\mathbf{m} = m'] && \text{(by definition of Shannon security)} \\
&= \Pr[E(\mathbf{k}, m) = c] \textstyle\sum_{m' \in M} \Pr[\mathbf{m} = m'] = \Pr[E(\mathbf{k}, m) = c]
\end{aligned}$$

Hence we have:
$\Pr[\mathbf{c} = c \wedge \mathbf{m} = m] = \Pr[\mathbf{c} = c] \Pr[\mathbf{m} = m]$
If we have an extra assumption that for every $c \in C$ we have $\Pr(c) > 0$ then :
$\Pr[\mathbf{c} = c \wedge \mathbf{m} = m] = \Pr[\mathbf{c} = c] \Pr[\mathbf{m} = m | \mathbf{c} = c] \rightarrow \Pr[\mathbf{m} = m | \mathbf{c} = c] = \Pr[\mathbf{m} = m]$
Hence Shannon security with this extra assumption imply Perfect security. without this extra assumption Shannon security does not necessarily imply perfect security. For example let the encryption of some $m_0 \in M$ to some c_0 be possible but the probability of this encryption be 0. and assume that the encryption of other members of M to c_0 is not possible. then Shannon security is possible because for any $m \in M$ we have $\Pr(Enc(m, \mathbf{k}) = c_0) = 0$. but it can not have perfect security because $\Pr(m_0 | c_0) = 1 \neq \Pr(m_0)$.

For the converse assume E is perfectly secure. we have
$\Pr[Enc(\mathbf{k},m)=c]Pr[\mathbf{m}=m]$

$=\Pr[Enc(\mathbf{k},m)=c\wedge\mathbf{m}=m]$ (by independence of k and m)

$=\Pr[Enc(\mathbf{k},\mathbf{m})=c\wedge\mathbf{m}=m]$

$=\Pr[\mathbf{c}=c\wedge\mathbf{m}=m]=\Pr[\mathbf{m}=m|\mathbf{c}=c]\Pr[\mathbf{c}=c]=\Pr[\mathbf{m}=m]\Pr[\mathbf{c}=c]$

If we have an extra assumption that for every $m\in M$ we have $\Pr(m)>0$ then :
$\Pr[\mathbf{c}=c]=\Pr[Enc(\mathbf{k},m)=c]$
Hence Perfect security with this extra assumption imply Shannon security. Similar argument as before shows that without this assumption Perfect security doesnt necesserily imply Shannon security.
b) Let message be $m\in\{0,1\}^n$ then generate some $k_1,k_2,k_3\in\{0,1\}^n$ by a uniform distribution on it. Share $m\oplus k_1\oplus k_2\oplus k_3$ with every one and share (k_1,k_2) with first one, (k_2,k_3) with second one and (k_1,k_3) with third one.

Problem 2

a) For $|K|\geq|M|$ there exists a system which advantage to any adversary is zero. So let $|K|\leq|M|$ and let the cipher space C be equal to message space M and E be a deterministic encryption system which its key generation chooses uniformly from K. let C_i be the members of C which m_i is encrypted to them for some $k\in K$. this system exists for example let $Enc(k,m)=m+k$ and $Dec(k,c)=c-k$. System is deteministic and decryptions works with probability 1, hence we have $|C_i|=|K|$.
Let A be an arbitrary adversary. assume it outputs $m_0,m_1\in M$. suppose $|C_0\cap C_1|=n$, Then we have $|C_1\backslash C_0|=|C_0\backslash C_1|=|K|-n$.
The adversary uses an algorithm, hence for every cipher c it gets as cipher thers exists a real number p(obviously dependeing to c) such that A chooses m_0 with probability p. Suppose A chooses m_0 with probability p_i if $c=a_i\in C_0\backslash C_1$ and with probability q_i if $c=b_i\in C_0\cap C_1$ and with probability s_i if $c=c_i\in C_1\backslash C_0$.
Now we calculate the advantage of A. key is chosen uniformly in K, hence the encryption of m_i is uniformly in C_i.
$advantage=|\Pr(m_0|m_0)-\Pr(m_0|m_1)|$

$=|\sum_{i=1}^{|K|-n}\Pr(c=a_i\wedge choose(m_0)|m_0)+\sum_{i=1}^{n}\Pr(c=b_i\wedge choose(m_0)|m_0)$
$-\sum_{i=1}^{n}\Pr(c=b_i\wedge choose(m_0)|m_1)-\sum_{i=1}^{|K|-n}\Pr(c=a_i\wedge choose(m_0)|m_1)|$

$= \frac{1}{|K|}|\sum_{i=1}^{|K|-n} p_i + \sum_{i=1}^{n} q_i - \sum_{i=1}^{n} q_i - \sum_{i=1}^{|K|-n} c_i| = \frac{1}{k}|\sum_{i=1}^{|K|-n} p_i - c_i|$

Hence the best adversary should choose for every i: $p_i = 1, c_i = 0$ and q_i doesnt really matter. Hence:

$advantage = \frac{|K|-n}{|K|}$

$n = |C_0 \cap C_1| = |K| - |C_1 \backslash C_0| \geq |K| - (|M| - |K|) = 2|K| - |M|$

$\rightarrow advantage \leq \frac{|M|-|K|}{|K|} = \frac{|M|}{|K|} - 1$

b) The Encryption system has the properties that we mentioned in the previous part hence:

$advantage \leq \frac{|M|}{|K|} - 1 = \frac{1}{1-\epsilon} - 1 = \frac{\epsilon}{1-\epsilon}$

For the second part let the key space be the set of n bits which the j first bits are not simultaneusly zero. we have $|K| = 2^n - 2^{n-j} = 2^n(1 - 2^{-j}) = (1-\epsilon)2^n$.

suppose an adversary outputs $m_0 = 000..0, m_1 = 111...1$ then C_0 is all of n bits which first j bits are not simultaneusly zero and C_1 is all of the n bits which first j bits are not simultaneusly one, hence:

$n = |C_0 \cap C_1| = 2^n - 2 \times 2^{n-j} \rightarrow advantage = \frac{|K|-n}{|K|} = \frac{2^{n-j}}{2^n(1-2^{-j})} = \frac{\epsilon}{1-\epsilon}$

Problem 3

Suppose a system has ϵ-security.

$\frac{\Pr(m_i) - \Pr(m_i|c_j)}{\Pr(m_i)} = -\beta_{ij} \rightarrow \Pr(m_i|c_j) = \Pr(m_i)(1+\beta_{ij}); |\beta_{ij}| \leq \epsilon < 1$

Let $m_i \in M$ with $\Pr(m_i) > 0$ and $c_0 \in C$ with $\Pr(c_0) > 0$ then we have

$\Pr(c_0|m_i) = \frac{\Pr(m_i|c_0)\Pr(c_0)}{\Pr(m_i)} = \Pr(c_0)(1+\beta_i) > \Pr(c_0)(1-\epsilon) \rightarrow \sum_i \Pr(c_0|m_i) = \infty$

Let X_i be the subset of key space which may encrypt m_i to c_0 then we have $\Pr(X_i) \geq \Pr(c_0|m_i)$. decryption should be done with probability 1 hence$X_i^{,}$ s are disjoint hence $\sum_i \Pr(X_i) \leq 1$ but we have $1 = \sum_i \Pr(X_i) \geq \sum_i \Pr(c_0|m_i) = \infty$ which is a contradiction. hence there is no system wich has ϵ-security.