Introduction to Modern Cryptography - EX. 1

Roi Koren 305428369
Noam Koren 204175004

November 7, 2018

1 Classical Cryptography

To break the substitution cipher we first made a frequency analysis of all letters in the given cipher. Since the two most frequent letters in the English alphabet ('E' and 'T') have a noticeable lead over the others, we inferred this will remain the same in the cipher, and substituted 'I' for 'E' and 'U' for 'T'.

Next, we searched for the most frequent letter between 'TE' in the text, knowing that most likely that letter would be 'H'. This was found to be 'Z'. Another common sequence is 'THA', which allowed us to find that 'B' is substituted for 'A'.

This was enough information to allow us to look at the received text and start making guesses, until eventually all letters were found.

The first twenty words of the deciphered text are:

> Years passed. The seasons came and went, the short animal lives fled by. A time came when there was no...

2 Perfect Secrecy

a Assume (E, D) is perfectly secret, and assume towards a contradiction that (E, D) is not perfectly indistinguishable, that is $\exists m_0, m_1 \in M$, and $\exists c \in C$ s.t $\Pr_{k \leftarrow K}[E_k(m_0) = c] < \Pr_{k \leftarrow K}[E_k(m_1) = c]$.

Set our distribution M to be uniform over $\{m_0, m_1\}$. From (E, D)'s perfect secrecy we get that -

$$\begin{aligned} 1/2 = \Pr[M = m_0] &= \Pr_{k \leftarrow K}[E_k(m_0) = c] \\ 1/2 = \Pr[M = m_1] &= \Pr_{k \leftarrow K}[E_k(m_1) = c] \end{aligned}$$

However, following our assumption, we get:

$$\Pr[M = m_0] = \Pr_{k \leftarrow K}[E_k(m_0) = c] < \Pr_{k \leftarrow K}[E_k(m_1) = c] = \Pr[M = m_1]$$

A contradiction. Hence if (E, D) is perfectly secret, then it is also perfectly indistinguishable.

b Assume (E, D) is perfectly indistinguishable, meaning

$$\forall m \neq m' \in M : \Pr_{k \leftarrow K}[E_k(m) = c] = \Pr_{k \leftarrow K}[E_k(m') = c]$$

$$\begin{aligned}
\Pr_{k\leftarrow K}[M=m|E_k(m)=c] &= \frac{\Pr[M=m]\cdot \Pr_{k\leftarrow K}[E_k(m)=c|M=m]}{\Pr[E_k(M)=c]}\\
&= \frac{\Pr[M=m]\cdot \Pr_{k\leftarrow K}[E_k(m)=c]}{\sum\limits_{x\in M}\Pr_{k\leftarrow K}[E_k(x)=c]\cdot \Pr[M=x]}\\
&= \frac{\Pr[M=m]\cdot \Pr_{k\leftarrow K}[E_k(m)=c]}{|M|\cdot \Pr_{k\leftarrow K}[E_k(m)=c]\cdot \frac{1}{|M|}} = \Pr[M=m]
\end{aligned}$$

This means that (E,D) is perfectly secret, and thus if (E,D) is perfectly indistinguishable, then it is also perfectly secret.

c Assume, similarly to part (a) of the question, that (E,D) is not perfectly indistinguishable, with the same m_0, m_1, c and set M in the same way.

Construct an adversary that presents his opponent with m_0, m_1. If the response he receives is c, the adversary answers 1. Otherwise it picks an answer at random from $\{0,1\}$. We get the following results:

$$\begin{aligned}
\Pr[b=b'] &= \Pr[b=b'|M=m_0]\cdot\Pr[M=m_0]\\
&+\Pr[b=b'|M=m_1]\cdot\Pr[M=m_1]\\
&= 1/2\cdot(\Pr[b=b'|M=m_0]+\Pr[b=b'|M=m_1])\\
\Pr[b=b'|M=m_1] &= \Pr[C=c|M=m_1]\cdot\Pr[b=b'|M=m_1,C=c]\\
&+\Pr[C\neq c|M=m_1]\cdot\Pr[b=b'|M=m_1,C\neq c]\\
&= \Pr[C=c|M=m_1]+1/2\cdot\Pr[C\neq c|M=m_1]\\
\Pr[b=b'|M=m_0] &= \Pr[C=c|M=m_0]\cdot\Pr[b=b'|M=m_0,C=c]\\
&+\Pr[C\neq c|M=m_0]\cdot\Pr[b=b'|M=m_0,C\neq c]\\
&= 1/2\cdot\Pr[C\neq c|M=m_0]\\
\Pr[b=b'] &= 1/2\cdot(\Pr[C=c|M=m_1]+1/2\cdot\Pr[C\neq c|M=m_1]\\
&+1/2\cdot\Pr[C\neq c|M=m_0])\\
&= 1/2\cdot(\Pr[C=c|M=m_1]+1/2\cdot(1-\Pr[C=c|M=m_1])\\
&+1/2\cdot\Pr[C\neq c|M=m_0])\\
&= 1/4+1/4\cdot(\Pr[C=c|M=m_1]+\Pr[C\neq c|M=m_0])\\
&> 1/4+1/4\cdot(\Pr[C=c|M=m_0]+\Pr[C\neq c|M=m_0])\\
&= 1/2
\end{aligned}$$

This result means that the adversary has a distinguishing advantage between m_0, m_1, and (E,D) is not adversarial indistinguishable. This means that if (E,D) is adversarial indistinguishable, then it is also perfectly indistinguishable.

3 One-Time Pad over Generic Groups

a To show perfect secrecy, we wish to show that for $m, m'; m \neq m'$:
$\Pr_k[E_k(m) = c] = \Pr_k[E_k(m') = c]$.
It holds that $\forall m \in S$:

$$\Pr_k[E_k(m) = c] = \Pr_k[k \oplus m = c] = \Pr_k[k \oplus m \oplus m^{-1} = c \oplus m^{-1}]$$
$$\Pr_k[E_k(m) = c] = \Pr_k[k = c \oplus m^{-1}] = \frac{1}{|S|}$$

Where we used the Associativity and Inverse properties of the S group, and assumed a uniform distribution of messages in S. This is true for every m, meaning this encryption scheme is a perfect cipher.

b Using this encryption scheme to encrypt multiple messages, an adversary may gather the following information. For $c_1 = E_k(m_1)$ and $c_2 = E_k(m_2)$:

$$c_1{}^{-1} \oplus c_2 = (m_1{}^{-1} \oplus k^{-1}) \oplus (k \oplus m_2) = m_1{}^{-1} \oplus m_2$$

4 Statistical Distance

a Let X and Y be defined as in the question.

$$\forall i \in \{1, ..., 12\}. \Pr[X = i] = \frac{1}{12}$$
$$\Pr[Y = 1] = 0$$
$$\Pr[Y = 2] = \Pr[Y = 12] = \frac{1}{36}$$
$$\Pr[Y = 3] = \Pr[Y = 11] = \frac{2}{36} = \frac{1}{18}$$
$$\Pr[Y = 4] = \Pr[Y = 10] = \frac{3}{36} = \frac{1}{12}$$
$$\Pr[Y = 5] = \Pr[Y = 9] = \frac{4}{36} = \frac{1}{9}$$
$$\Pr[Y = 6] = \Pr[Y = 8] = \frac{5}{36}$$
$$\Pr[Y = 7] = \frac{6}{36} = \frac{1}{6}$$
$$\Delta(X, Y) = 1/2 \cdot \sum_{s \in S} |\Pr[X = s] - \Pr[Y = s]| =$$
$$\frac{1}{2} \cdot \left(\frac{1}{12} + 2 \cdot \frac{1}{18} + 2 \cdot \frac{1}{36} + 2 \cdot \frac{1}{36} + 2 \cdot \frac{1}{18} + \frac{1}{12}\right) = \frac{3 + 4 + 2 + 2 + 4 + 3}{72} = \frac{1}{4}$$

Construct an adversary A, so that $A(s) = 1$ if $s \in \{5, 6, 7, 8, 9, 10\}$, $A(s) = 0$ if $s \in \{1, 2, 3, 4, 11, 12\}$.

$$\Delta_A(X, Y) = |\Pr[A(X) = 1] - \Pr[A(Y) = 1]| =$$

$$|\sum_{x \in S} \Pr[A(x) = 1|X = x] \cdot \Pr[X = x] - \sum_{y \in S} \Pr[A(y) = 1|Y = y] \cdot \Pr[Y = y]| =$$

$$|\frac{1}{2} - \left(\frac{4}{36} + \frac{5}{36} + \frac{6}{36} + \frac{5}{36} + \frac{4}{36} + \frac{3}{36}\right)| = |\frac{1}{2} - \frac{27}{36}| = | - \frac{9}{36}| = \frac{1}{4}$$

b Let X, Y be discrete random variables over a set S, A a distinguisher.

$$\begin{aligned}
\Delta_A(X, Y) &= |\Pr[A(X) = 1] - \Pr[A(Y) = 1]| \\
&= |\sum_{s \in S} \Pr[A(s) = 1|X = s] \cdot \Pr[X = s] \\
&- \sum_{s \in S} \Pr[A(s) = 1|Y = s] \cdot \Pr[Y = s]| \\
&= |\sum_{s \in S} (\Pr[A(s) = 1|X = s] \cdot \Pr[X = s] \\
&- \Pr[A(s) = 1|Y = s] \cdot \Pr[Y = s])| \\
&= |\sum_{s \in S} \Pr[A(s) = 1] \cdot (\Pr[X = s] - \Pr[Y = s])\,| \\
&\leq^{(*)} |\frac{1}{2} \cdot \sum_{s \in S} (\Pr[X = s] - \Pr[Y = s])| \\
&\leq \frac{1}{2} \cdot \sum_{s \in S} |\Pr[X = s] - \Pr[Y = s]| = \Delta(X, Y)
\end{aligned}$$

In $(*)$ we used the fact that $\Pr_{s \in S}[A(s) = 1] \leq \frac{1}{2}$, since an adversary could at worst flip a coin to choose his response, and he would be correct half of the times.

As we saw in part (a) of the question, we can construct an adversary A, whose distinguishing advantage is equal to $\Delta(X, Y)$.

5 Computational Indistinguishability and the Hybrid Argument

a We'll prove by contradiction. Suppose there exists a t-sized adversary A that can distinguish between (X, X) and (Y, Y):

$$2\epsilon \leq |\Pr_{x_1,x_2\leftarrow X}(A(x_1,x_2)=1) - \Pr_{y_1,y_2\leftarrow Y}(A(y_1,y_2)=1)|$$

$$= |\Pr_{x_1,x_2\leftarrow X}(A(x_1,x_2)=1) - \Pr_{\substack{x\leftarrow X\\ y\leftarrow Y}}(A(x,y)=1) + \Pr_{\substack{x\leftarrow X\\ y\leftarrow Y}}(A(x,y)=1) - \Pr_{y_1,y_2\leftarrow Y}(A(y_1,y_2)=1)|$$

$$\leq |\Pr_{x_1,x_2\leftarrow X}(A(x_1,x_2)=1) - \Pr_{\substack{x\leftarrow X\\ y\leftarrow Y}}(A(x,y)=1)| + |\Pr_{\substack{x\leftarrow X\\ y\leftarrow Y}}(A(x,y)=1) - \Pr_{y_1,y_2\leftarrow Y}(A(y_1,y_2)=1)|$$

Since the sum must be greater than 2ϵ, one of these two operands must be greater than ϵ. w.l.g we'll assume it's the first operand -

$$|\Pr_{x_1,x_2\leftarrow X}(A(x_1,x_2)=1) - \Pr_{\substack{x\leftarrow X\\ y\leftarrow Y}}(A(x,y)=1)| \geq \epsilon$$

An adversary B for X, Y will have the following algorithm for a given input c:

- Choose a random x from X
- Return $A(x, c)$

B is of size t, and can distinguish between X and Y with a probability greater than ϵ, and we have reached a contradiction, meaning $(X, X) \approx_{t,2\epsilon} (Y, Y)$.

b In a similar way we can prove that $X^s \approx_{t,s\epsilon} Y^s$. For a t-sized adversary A that can distinguish between X^s and Y^s:

$$s\epsilon \leq |\Pr_{\vec{x}\leftarrow X^s}(A(x_1,...,x_s)=1) - \Pr_{\vec{y}\leftarrow Y^s}(A(y_1,...,y_s)=1)|$$

We'll define $H^i = (X_1, ..., X_i, Y_{i+1}, ..., Y_s)$:

$$s\epsilon \leq |\Pr(A(H^s)=1) - \Pr(A(H^0)=1)|$$

$$= |\Pr(A(H^s)=1) - \sum_{i=1}^{s-1}\Pr(A(H^i)=1) + \sum_{i=1}^{s-1}\Pr(A(H^i)=1) - \Pr(A(H^0)=1)|$$

$$= |\sum_{i=0}^{s-1}\Pr(A(H^i)) - \sum_{i=0}^{s-1}\Pr(A(H^{i+1}))| = |\sum_{i=0}^{s-1}(\Pr(A(H^i)) - \Pr(A(H^{i+1})))|$$

$$\leq \sum_{i=0}^{s-1}|\Pr(A(H^i)) - \Pr(A(H^{i+1}))|$$

Again, we have s operands whose sum is greater than $s\epsilon$. One of them must be greater than ϵ. w.l.g we'll assume it's the first operand -

$$|\Pr(A(H^0)=1) - \Pr(A(H^1)=1)| =$$
$$|\Pr(A(x_1,...,x_s)=1) - \Pr(A(x_1,y_2,...,y_s)=1)| \geq \epsilon$$

An adversary B for X, Y will have the following algorithm for a given input c:

- Choose a random x from X, and $s-2$ random y's from Y
- Return $A(x, y_1, ..., y_{s-2}, c)$

B is of size t, and can distinguish between X and Y with a probability greater than ϵ, and we have reached a contradiction, meaning $X^s \approx_{t,s\epsilon} Y^s$.

c G is a PRG, meaning $G \approx_{t,\epsilon} U_{n+1}$. Where U_{n+1} is the uniform distribution. We can model $G'(x_1, ..., x_{p(n)}) = G(x_1)||...||G(x_{p(n)})$ as taking $p(n)$ independent elements, as in section B. Using the result from that section we get that $G' \approx_{t,p(n)\cdot\epsilon} U_{n+1}^{p(n)}$, and that G' is a PRG.

6 Euclidean Algorithm

Roi

$$\begin{gathered}
r_{-1} = 305428369, r_0 = 456 \\
r_1 = r_{-1} \mod r_0 = 25 \\
r_2 = r_0 \mod r_1 = 6 \\
r_3 = r_1 \mod r_2 = 1 \\
r_4 = r_2 \mod r_3 = 0 \\
gcd(305428369, 456) = 1
\end{gathered}$$

The computation took 4 steps.

Noam

$$\begin{gathered}
r_{-1} = 204175004, r_0 = 456 \\
r_1 = r_{-1} \mod r_0 = 92 \\
r_2 = r_0 \mod r_1 = 88 \\
r_3 = r_1 \mod r_2 = 4 \\
r_4 = r_2 \mod r_3 = 0 \\
gcd(204175004, 456) = 4
\end{gathered}$$

Here too, the computation took 4 steps.