IS53012B/A Computer Security

Dr Ida Pu

Room 10, 29 St James
Goldsmiths, University of London

2018-19 (since 2007)

Part I

Workshop

Week 1 Homework

1. Given the probability distributions of two event sources $P_1 = [0.3, 0.2, 0.4, 0.1]$, and $P_2 = [0.3, 0.1, 0.5, 0.1]$, which source is more random on average? Justify your answer.
2. What can you say about a binary source with two events only?

Week 1 Homework Solutions

1. Given the probability distributions of two event sources $P_1 = [0.3, 0.2, 0.4, 0.1]$, and $P_2 = [0.3, 0.1, 0.5, 0.1]$, which source is more random on average? Justify your answer.

   $$H_1 = -\sum(P_1. * log2(P_1)) \approx 1.85$$

   $$H_2 = -\sum(P_2. * log2(P_2)) \approx 1.69$$

   As $H_1 > H_2$, the source with P_1 probability distribution is more random.
2. What can you say about a binary source with two events only?

   Hint: Plot the entropy against the binary probability distribution $(p, 1-p)$, i.e. (p_1, p_2), where $p_1 + p_2 = 1$.

Week 2 Homework

John proposes a cryptosystem that is based on one-time key pad and requires no key exchange. It works as follows: If she wants to send Bob a message m, Alice generates her key k_a, a sequence of random bits (the same length as m), computes $c = m \oplus k_a$ and sends c to Bob, where $\oplus$ represents the bitwise XOR operation. On receipt of c, Bob generates his own random bits k_b of same length, computes $d = c \oplus k_b$ and sends d to Alice. On receipt of d, Alice computes $e = d \oplus k_a$ and sends e to Bob. On receipt of e, Bob computes $e \oplus k_b$ for the last time.
Analyse John's cryptosystem and conclude whether John's cryptosystem works.

Week 2 Homework (continued)

The following format may be adopted to help demonstrate what happens with the plaintext m that from Alice to Bob, where "??" parts are for you to figure out. Each of the 3 columns shows the series of the values (or texts) visible by Alice, Bob or Charlie.

$$\begin{tikzcd}
\text{Alice} & \text{Charlie} & \text{Bob} \\
\text{m} \arrow[d] & & \\
?? \arrow[r] & ?? \arrow[r] & ?? \arrow[d] \\
?? \arrow[d] & ?? \arrow[l] \arrow[d] & ?? \arrow[l] \\
?? \arrow[d] & ?? & \\
?? \arrow[r] & ?? \arrow[r] \arrow[d] & ?? \arrow[d] \\
 & ?? & ??
\end{tikzcd}$$