IS53012B/A Computer Security

Dr Ida Pu

Room 10, 29 St James
Goldsmiths, University of London

2018-19 (since 2007)

Part I

Workshop

Outline

1. Week 2 Homework

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.

$$
\begin{array}{ccccc}
\text{Alice} & & \text{Charlie} & & \text{Bob} \\
\hline
\text{m} & & & & \\
\downarrow & & & & \\
?? & \rightarrow & ?? & \rightarrow & ?? \\
 & & & & \downarrow \\
?? & \leftarrow & ?? & \leftarrow & ?? \\
\downarrow & & \downarrow & & \\
?? & & ?? & & \\
\downarrow & & & & \\
?? & \rightarrow & ?? & \rightarrow & ?? \\
 & & \downarrow & & \downarrow \\
 & & ?? & & ??
\end{array}
$$

How does it work?

Alice		Bob
m		
$\downarrow$		
$m \oplus k_a$	$\rightarrow\rightarrow$	$m \oplus k_a$
		$\downarrow$
$m \oplus k_a \oplus k_b$	$\leftarrow\leftarrow$	$m \oplus k_a \oplus k_b$
$\downarrow$		
$m \oplus k_a \oplus k_b \oplus k_a = m \oplus k_b$	$\rightarrow\rightarrow$	$m \oplus k_b$
		$\downarrow$
		$m \oplus k_b \oplus k_b = m$

Charlie may overhear

Alice		Charlie		Bob
m				
$\downarrow$				
$m \oplus k_a$	$\rightarrow$	$m \oplus k_a$	$\rightarrow$	$m \oplus k_a$
				$\downarrow$
$m \oplus k_a \oplus k_b$	$\leftarrow$	$m \oplus k_a \oplus k_b$	$\leftarrow$	$m \oplus k_a \oplus k_b$
$\downarrow$		$\downarrow$		
$m \oplus k_a \oplus k_b \oplus k_a$		$(m \oplus k_a) \oplus (m \oplus k_a \oplus k_b) = k_b$		
$\downarrow$				
$m \oplus k_a \oplus k_b \oplus k_a = m \oplus k_b$	$\rightarrow$	$m \oplus k_b$	$\rightarrow$	$m \oplus k_b$
		$\downarrow$		$\downarrow$
		$k_b \oplus m \oplus k_b = m$		$m \oplus k_b \oplus k_b = m$