AARHUS UNIVERSITY

Security - Handin 1

Peter Burgaard - 201209175

April 14, 2015

WHAT IS THE VALUE OF BIT 20 IN THE PAYMENT ORDER? Since bit can have two value 0 and 1, and we have 21 of these (we also count bit 0) it can be written as:

$$\overbrace{100000000000000000000}^{\text{binary}} = 2^{20} = 1048576$$

SHOW HOW HE CAN MODIFY THE ENCRYPTED PAYMENT ORDER IN SUCH A WAY THAT HE WILL RECEIVE MORE THAN A MILLION KR. EXTRA NEXT MONTH. Since we assume "he makes less that a million kr. pr month" we know that the maximum binary number that can be used in the salary massage m is at most a 20 bit number, which mean 21st bit is 0. Since the one-time pad xors (⊕) the massage with a random key k of the same lenght as the massage, and we know that the 21st bit in m is 0, we check the ciphertext c for its 21st bit. If c's 21st bit is 0, we know k's 21st bit is also 0, due to ⊕ truth table.

$$\oplus = \left\{ \begin{array}{c|c|c} m_i \text{ bit} & k_i \text{ bit} & c_i \text{ bit} \\ \hline 1 & 1 & 0 \\ \hline 1 & 0 & 1 \\ \hline 0 & 1 & 1 \\ \hline 0 & 0 & 0 \end{array} \right.$$

Likewise if c's 21st bit is 1, we know that k's 21si is 1. All we have to do to secure the million dollar transfer is to flip c's 21st bit, because this will result in m's 21st bit being flipped, which adds 1048576kr extra to transfer. This can only be done because we know that m's 21st bit is a 0. If we didn't have the knowledge about the salaries size, we would have no idea about its binary value, and therefore flipping the bit would be a 50/50 chance.

IS THE SECURITY PROBLEM YOU HAVE SEEN HERE A CONFIDENTIALITY PROBLEM OR AN AUTHENTICITY PROBLEM? This would be a confidentiality problem, due to the fact that we have no idea about what this mans salary is due to the one-time pad encryption. This is clearly shown by the above assignment, because the only thing we can assume is the salary being less that a million. Other than that, we have no idea what it is.

THE NOTES CLAIM THAT THE ONE-TIME PAD CANNOT BE BROKEN, AND YET WE HAVE IDENTIFIED A SECURITY PROBLEM HERE. WHY IS THIS NOT A CONTRADICTION? The poor security officer, have unfortunately mixed up some concepts. What the officer noted in his threat model would've been security against authenticity attacks, but clearly the system isn't. This is because the one-time pad is used to secure data against confidentiality attacks. "Whether a given system is secure or not can depend dramatically on which threat model is considered"[1].

[1] Damgård, Ivan "An introduction to some Basic Concepts in IT Security and Cryptography", Threat Model, p. 3