Homework 5

Ally Smith

April 7, 2022

Problem 1

Please read this short article about Bruce Schneier's comments on FREAK: `https://www.schneier.com/blog/archives/2015/03/freak_security_.html`

He considered FREAK as one type of **"Security Rollback"** attacks, a generic problem with government-mandated backdoors, key escrow, "golden keys," etc. He stated that "We don't know how to design a third-party access system that checks for morality; once we build in such access, we then have to ensure that only the good guys can do it. And we can't." He further justified his opinion by quoting the Economist: "...mathematics applies to just and unjust alike; a flaw that can be exploited by Western governments is vulnerable to anyone who finds it."

What does the acronym FREAK represent and what is the essential problem of this flaw? Do you agree or disagree with Bruce's opinion on FREAK and Security Rollback attacks in general, and why? (Your answer to this question should have **at least 60 words**).

FREAK stands for 'Factoring Attack on RSA-EXPORT Keys', and it represents a more general kind of attack. Many older systems often retain less secure encryption methods as a form of backwards compatibility. However, in a security rollback attack, the attacker forces the system to use the weaker algorithm, allowing the system to be exploited. Additionally, these attacks can rely on 'backdoors' or 'golden keys' to enter the system. As a result, Schneier argues that we shouldn't include backdoors or the likes in any form. I agree with Schneier that this is a glaring security issue, but it does seem like a complicated issue, as older systems need those less secure algorithms to function.

Problem 2

Consider an ElGamal Message Exchange with a common prime $q = 71$ and a primitive root $a = 7$. Meanwhile, we know that Alice has the public key $Y_a = 3$, and Bob wants to encrypt a message M to send to Alice.

- If Bob chooses the random integer $k = 2$, what is the ciphertext of $M = 30$?

  $K = Y_a^k \pmod q$
  $K = 3^2 \pmod{71} \equiv 6$

  $C_1 = a^k \pmod q$
  $C_1 = 7^2 \pmod q \equiv 49$

  $C_2 = KM \pmod q$
  $C_2 = 6 \times 30 \pmod{71} \equiv 38$

  $C = \langle C_1, C_2 \rangle = \langle 49, 38 \rangle$

- If Bob now chooses a different value of k so that the encoding of $M = 30$ is $C = (59, C_2)$, what is the integer C_2? Hint: you first need to derive the value of k.

  $59 \equiv 7^k \pmod{71}$
  $k = 3$

  $K = Y_a^k \pmod q$
  $K = 3^3 \pmod{71} \equiv 9$

  $C_2 = KM \pmod q$ $C_2 = 9 \times 30 \pmod{71}$

  $C_2 = 57$

Problem 3

It is possible to use a hash function to construct a block cipher with a structure similar to DES. Because a hash function is one way, and a block cipher must be reversible, how is it possible?

This is possible to implement because DES follows a Feistel structure. You can use the hash function as the function in the cipher. This works for both encryption and decryption, as the function applies to each of them in a Feistel structure.

Problem 4

Now consider the opposite problem: using an encryption algorithm to construct a one-way hash function. Consider using RSA with a known key. Then process a message consisting of a sequence of blocks as follows: Encrypt the first block, XOR the results with the second block, and encrypt again, etc. Show that this scheme is not secure by solving the following problem. Given a two-block message B_1, B_2, and its hash:

$$RSAH(B_1, B_2) = RSA(RSA(B_1) \oplus B_2)$$

Given an arbitrary block C_1, please construct C_2 such that $RSAH(C_1, C_2) = RSAH(B_1, B_2)$. Thus, the hash function does not satisfy weak collision resistance.

$$\begin{aligned}
RSA(RSA(B_1) \oplus B_2) &= RSA(RSA(C_1) \oplus C_2) \\
RSA(B_1) \oplus B_2 &= RSA(C_1) \oplus C_2 \\
RSA(B_1) \oplus B_2 \oplus RSA(C_1) &= RSA(C_1) \oplus C_2 \oplus RSA(C_1) \\
RSA(B_1) \oplus B_2 \oplus RSA(C_1) &= C_2
\end{aligned}$$