Tutorial 3 - Solutions

Computer Security
School of Informatics
University of Edinburgh

In this third tutorial for the Introduction to Computer Security course we delve deeper into Cryptography. The tutorial consists partly of questions from past years exams.

You are free to discuss these questions and their solutions with fellow students also taking the course, and also to discuss in the course forum. Bear in mind that if other people simply tell you the answers directly, you may not learn as much as you would by solving the problems for yourself; also, it may be harder for you to assess your progress with the course material.

1 Historical Cryptography

The Scytale cipher was used for military purposes in ancient Sparta. The encryption is done by wrapping a long strip of parchment around a baton and writing the message horizontally, letter by letter on adjacent parts of the strip. The strip is then unwound, delivered to the recipient and wound around a similar baton so that the letters align correctly and the original message can be read.

1. What is the key for encryption? For decryption?

   Solution

   The key is the diameter of the baton in both cases.

2. Is the encryption scheme symmetric or asymmetric? Why?

   Solution

   It is symmetric, since the same key is used for encryption and decryption.

2 Cryptographic Proofs, part 2

Prove that the RSA encryption scheme is consistent: Given a public - secret keypair $(n, e), d$, it is

$$Dec_{RSA}\left(d, Enc_{RSA}\left((n, e), m\right)\right) = m \pmod{n} \ .$$

Hint: Use Euler's theorem.

Solution

It is

$$ed = 1 \pmod{\phi(n)} \Rightarrow \exists a \in \mathbb{N} : ed = 1 + a\phi(n) \quad . \tag{1}$$

Thus

$$\begin{gathered}
Dec_{RSA}\left(d, Enc_{RSA}\left((n, e), m\right)\right) = \\
\left(m^e\right)^d \mod n = \\
m^{ed} \mod n \overset{(1)}{=} \\
m^{a\phi(n)+1} \mod n = \\
m^{a\phi(n)} m \mod n \overset{Euler}{=} \\
m \mod n \ .
\end{gathered}$$

3 Hash functions, part 2

Let $\mathcal{M} = \{0,1\}^*$ and $\mathcal{T} = \{0,1\}^n$ for some integer n. Suppose $h : \mathcal{M} \to \mathcal{T}$ is one-way. Is h also collision resistant? If so, explain why. If not, give an example of a one-way function that is not collision resistant. Suppose the DLOG assumption is true.

Solution

Let p a large prime and g a generator of $\mathbb{Z}_p$. Let h be the function $h(x) = g^x \mod p$. This function is one way from the DLOG assumption: inverting exponentiation over a discrete group is computationally hard. However, this function is not collision resistant. Indeed, if we choose x_1 and $x_2 = x_1 + (p-1)$, then

$$g^{x_2} = g^{x_1+(p-1)} = g^{x_1} g^{(p-1)} = g^{x_1} \pmod p \ .$$

4 Digital Signatures

Let H be a collision-resistant hash function. The ElGamal signature scheme is as follows:

- **Key generation:** Let p and Z_p^* a multiplicative group with a generator g. Alice picks a random integer x such that $1 < x < p-2$. This is her private key, used for signing. She then publishes $y = g^x \mod p$. This is the corresponding public key, used for signature verification.

- **Signature generation:** In order to sign a message m such that $0 \leq m < p$ with the private key x, Alice:

  1. Chooses a random k such that $1 < k < p-1$ and $\gcd(k, p-1) = 1$.
  2. Computes $r = g^k \pmod p$.
  3. Computes $s = (H(m) - xr)\, k^{-1} \pmod{p-1}$.

  The pair (r, s) is Alice's signature on m.

- **Signature verification:** In order to verify that a signature (r, s) corresponds to a message m using the public key y, Bob checks that the following condition holds:

$$g^{H(m)} \equiv y^r r^s \pmod{p} \ .$$

How the private key x can be compromised if the random value k is used in signing two different messages m_1, m_2?

Solution

Assuming that $s_1 - s_2$ and r are invertible modulo $p - 1$, the adversary can calculate x as follows:

$$\begin{aligned} k &= \left(H\left(m_1\right) - H\left(m_2\right)\right)\left(s_1 - s_2\right)^{-1} \pmod{p-1} \\ x &= \left(H\left(m_1\right) - ks_1\right) r^{-1} \pmod{p-1} \end{aligned}$$

In case the assumption does not hold, we can solve for k the congruence

$$k\left(s_1 - s_2\right) = \left(H\left(m_1\right) - H\left(m_2\right)\right) \pmod{p-1} \ .$$

This will produce $\gcd\left(s_1 - s_2, p - 1\right)$ solutions. Some solution will be such that

$$r = g^k \pmod{p-1} \ .$$

Then we can solve for x the congruence

$$xr = \left(H\left(m_1\right) - ks_1\right) \pmod{p-1} \ .$$

The private key will be some solution amongst the $\gcd\left(r, p - 1\right)$ solutions such that

$$y = g^x \pmod{p-1} \ .$$