Security on the Internet, summer 2007

MICHAEL NÜSKEN, DANIEL LOEBENBERGER

13. Exam preperation sheet
No hand in, voluntary

Exercise 1 (A power). (5 points)

Compute $3^{1\,987\,654\,321\,234\,567\,891} \text{ rem } 101$. (Explain your procedure.) 5

Exercise 2 (Fermat). (5 points)

Let p be a prime. Prove Fermat's little theorem, ie. for all $a \in \mathbb{Z}_p^\times$ we have 5

$$a^{p-1} \equiv 1 \pmod{p}.$$

Exercise 3 (Weak ciphers). (5 points)

Consider the following improvement of the Caesar cipher, namely the cipher over $P = C = \mathbb{Z}_{26}$ with keyspace $K = \{\pi \colon P \to C \,|\, \pi \text{ bijective}\}$ where the encryption function is given by

$$\text{enc}_\pi \colon \begin{array}{ccc} P & \longrightarrow & C, \\ x & \longmapsto & \pi(x). \end{array}$$

(i) Define the decryption function for the improved Caesar cipher. Why is it well defined? 1

(ii) Assume you have intercepted a long message that was encrypted using this improved Caesar cipher. How would you attempt to find the key? Discuss carefully. Classify the attack (ciphertext-only, known plaintext, chosen plaintext). 2

(iii) Consider now the combination of the improved Caesar cipher with another improved Caesar cipher. (More precisely the ciphertext of the first cipher is input for the second). Is this combination stronger than a single application of an improved Caesar cipher? Prove your claim. 2

Exercise 4 (Touching $\mathbb{F}_8$). (12+3 points)

Consider polynomials of degree less than 3 over the field $\mathbb{F}_2$. Define addition and multiplication of them modulo the polynomial $X^3 + X + 1 \in \mathbb{F}_2[X]$.

(i) Proof that $X^3 + X + 1$ is irreducible over $\mathbb{F}_2$. 2

(ii) Write down the complete list of elements. 2

(iii) Write down the multiplication table. [3]

(iv) We can now consider polynomials over $\mathbb{F}_8$: $T^3 + T + 1 \in \mathbb{F}_8[T]$ is such a polynomial. Factor it (over $\mathbb{F}_8$). [5]

(v) Factor $T^3 + T^2 + 1$. [+3]

Exercise 5 (Computing in $\mathbb{F}_{256}$). (7 points)

Let $a = 42$ and $b = 56$. Just as in AES interpret a and b as elements of $\mathbb{F}_{256}$, where $\mathbb{F}_{256}$ is represented by polynomials of degree less than 8 and the operations are modulo $X^8 + X^4 + X^3 + X + 1$.

(i) Compute $a + b$ in $\mathbb{F}_{256}$. [2]

(ii) Compute $a \cdot b$ in $\mathbb{F}_{256}$. [2]

(iii) Compute $1/a$ in $\mathbb{F}_{256}$. [3]

Exercise 6 (AES). (6 points)

Consider the Advanced Encryption Standard (AES):

(i) Describe the toplevel view of AES. [2]

(ii) Why do you believe AES is secure/insecure? State and argue. [4]

Exercise 7 (Diffie Hellman key exchange). (5+1 points)

Perform a toy example of a Diffie Hellman key exchange: Fix $p = 61$ and $g = 2 \in \mathbb{Z}_p^\times$.

(i) Show that the order of g is 60. [1]

[If you are clever then you only need to calculate g^{30}, g^{20}, and g^{12}.] [+1]

(ii) Choose $x \in \mathbb{Z}_p$ (take $x \notin \{0, 1\}$ to get something interesting) and calculate $h_A := g^x$. [1]

(iii) Choose $y \in \mathbb{Z}_p$ (take $y \notin \{0, 1, x\}$ to get something interesting) and calculate $h_B := g^y$. [1]

(iv) Now compute h_B^x and h_A^y and compare. [2]

Exercise 8 (DHP versus DLP). (4 points)

We are given a group G (as for example $\mathbb{Z}_p^\times$) and some element $g \in G$.

[1] (i) Formulate the discrete logarithm problem.

[1] (ii) Formulate the Diffie-Hellman problem.

[2] (iii) Reduce the latter to the former.

Exercise 9 (ElGamal practice). (6 points)

This is a toy example of ElGamal signing and signature verification. Let the key of a domain be given by $p = 10^{20} + 39$, $G = \mathbb{Z}_p^\times$, $g = 3 \bmod p \in G$, let $\ell = p - 1$ be the order of g. Use a system capable of computing with large numbers for solving the following problems:

(i) Check that p is prime and g generates the multiplicative group $\mathbb{Z}_p^\times$. [1]

(ii) Let m be the numerical value of the message *sign* (in a suitable encoding, say based on the ASCII values). Choose a secret key $\alpha \in \mathbb{Z}_\ell$ on behalf of the signer A and let $a = g^\alpha$ be his public key. Produce a signature (m, b, γ) of the text m. [2]

(iii) Use the public key a in order to verify the signed text (m, b, γ). [2]

(iv) Repeat the last two items 10 times, using each time different random keys α, while the same message should be used several times. [1]

Exercise 10 (ElGamal signatures). (8 points)

We choose a prime number $p = 12347$ and the group $G = \mathbb{Z}_p^\times$. We use $\alpha = 9876$ as the secret part of the key $K = (p, g, a, \alpha)$. The message ξ to be signed consists of the last four digits of your student registration number.

(i) Show that $g = 2$ generates G. Thus the order ℓ of g equals $p - 1 = \#G$. [2]

We now define the structureless map $^*\colon G \to \mathbb{Z}_\ell$ by mapping $k \bmod p$ to $k \bmod \ell$ for $k \in \mathbb{N}_{<p}$.

(ii) Compute $a = g^\alpha \in G$. [2]

(iii) Compute the signature $\mathrm{sig}_K(\xi, \beta) = (\xi, b, \gamma)$. Here $b = g^\beta$ in G and $\gamma = (\xi - \alpha b^*)/\beta$ in $\mathbb{Z}_\ell$. [2]

(iv) Verify your signature (without using secret information like α and β!). [2]

Exercise 11 (A hash function?). (5 points)

Let p be a prime and fix $c \in \mathbb{Z}_p^\times$. Consider the following definition of a hash function: The compression function is given by

$$f\colon \begin{array}{ccc} \mathbb{Z}_p \times \mathbb{Z}_p & \longrightarrow & \mathbb{Z}_p, \\ (x,y) & \longmapsto & x \cdot y + c \end{array}$$

The actual hash function $H\colon \left(\mathbb{Z}_p^\times\right)^* \to \mathbb{Z}_p$ is given by $H(x) = f(H(x'), x_\ell)$ for $x = (x', x_\ell)$ with $x_\ell \in \mathbb{Z}_p^\times$, $x' \in \left(\mathbb{Z}_p^\times\right)^*$ and $H() = 0$. In particular $H(x) = f(1, x)$ for $x \in \mathbb{Z}_p^\times$ and $H((x_0, x_1, x_2)) = f(f(f(1, x_0), x_1), x_2)$ for $x_0, x_1, x_2 \in \mathbb{Z}_p^\times$.

[2] (i) Given c find a collision.

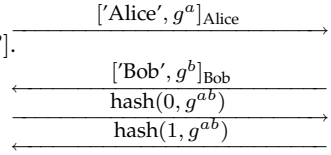
[3] (ii) Homer Simpson wants to take the above hash function to generate a digital signature (for example an ElGamal signature). Explain to him why he should not use it.

Exercise 12 (Key exchange threats). (6 points)

Consider the following signed key exchange scheme:

Protocol. Signed and acknowledged Diffie-Hellman key exchange.

1. Alice chooses $a \in \mathbb{N}_{<\#G}$, computes g^a and signs $['\text{Alice}', g^a]$.
2. Bob chooses $b \in \mathbb{N}_{<\#G}$, computes g^b and signs $['\text{Bob}', g^b]$.
3. Alice computes $(g^b)^a = g^{ab}$ and a hash.
4. Bob computes $(g^a)^b = g^{ab}$ and a hash.



As you have certainly guessed, $[\text{text}]_{\text{Alice}}$ denotes the text plus a signature by Alice on it.

[2] (i) Explain how a woman in the middle attack is foiled here.

[2] (ii) Does this protocol guarantee that Alice is live or could this just be a replay? Consider the case that Bob's temporary public key g^b is constant for some time.

[2] (iii) Explain how to 'heal' this deficiency (without forcing Bob to use a new b each time).

Exercise 13 (Types of Attacks). (5 points)

[5] Assume you want to design some protocol for secure communication. To do so you have to consider various types of attacks that are possible. Describe two of them and argue which countermeasures can be included in your design.

Exercise 14 (Secure communication). (10 points)

[10] Explain what is important to establish and maintain a secure connection between two entities in the Internet.