INF143A 22V Applied Cryptography
Second mandatory assignment

Nikolay Kaleyski

March 17, 2022

1 General information

- **Deadline:** The assignment is due on April 4, 2022.
- **Submission:** A copy of the solution should be uploaded to mitt, under the "Assignments" tab.
- **Score:** The mandatory assignment accounts for 15% of the final grade.
- **Collaboration:** You can freely discuss the assignment with each other, but the solutions must be prepared individually; plagiarism will result in all involved parties failing the assignment.

NB: Some of the problems (problem 2 and problem 5) have two variants; one of them is more "mathematical" while the other is more "implementational". You should choose and solve one of the two variants. Solving both variants will not give you any bonus points.

2 Problems

3 Number theory

Problem 1. ***15%*** *Find the last two digits of the number* $98765432^{12345678987654321}$.

Problem 2. ***20%*** *(variant A) Implement a primality test, e.g. the Fermat primality test or the Miller-Rabin primality test. Use it to find a prime number p with exactly d bits, where:*

- $d = 500$*;*
- $d = 671$*;*
- $d = 1024$*.*

Problem 2. ***20%*** *(variant B)*

- *Show that if* $x^2 \equiv y^2 \mod n$ *and* $x \not\equiv \pm y \mod n$*, then* $\gcd(x + y, n)$ *is a non-trivial factor of* n*.*

- *Consider* $n = 131981$. *Using the fact that for any* $x, y \in \{18504, 43380, 88601, 113477\}$ *we have* $x^2 \equiv y^2 \mod n$, *find the prime factorization of* n.
- *Consider* $n = 110732059$. *Again, for any* $x, y \in \{118925, 15192399, 18066813, 33140287, 77591772, 92665246, 95539660, 110613134\}$ *we have* $x^2 \equiv y^2 \mod n$, *find the prime factorization of* n.

4 Asymmetric encryption

Problem 3. ***20%*** *Suppose the RSA encryption scheme is used with the public key* $(n, e) = (15151, 17)$, *and suppose that you have intercepted the ciphertext* $y = 832$.

- *Find the prime factorization of* n, *i.e. find the primes* p, q *such that* $n = pq$;
- *compute* $\varphi(n)$;
- *using the above, find the private key* d;
- *using the private key, decrypt the ciphertext* y.

5 Digital signatures

Problem 4. ***25%*** *Consider the Elgamal digital signature scheme. Suppose during key generating we have selected*

$$p = 172471720944269739125606601541029487739340755626635$$
$$772583971303759438419175772663669593721846550197442744 4$$
$$696560806029466449270619511116886372753628036601400058 4$$
$$150943685841718789409496916181301383172231577618592484 2$$
$$099093899593568334696592964516617033076246061593684511 5$$
$$503447119631130624752716156631640609 97$$

and

$$g = 3.$$

Suppose the secret key is $d = 333$.

- *Compute the public key* (p, g, β).
- *Consider the message* $x = A3FB8FCE$ *(32 bits). Show how it can be represented as an integer modulo* p.
- *Sign the message* x, *i.e. compute the signature* $(x, (r, s))$.
- *Show how the signature is verified.*

6 Boolean functions

Problem 5. ***20%*** *(variant A) The so-called Gold function* $f(x) = x^3$ *in* $\mathbb{F}_{2^n}$ *(that is, as an* (n, n)*-function) is known to have differential uniformity equal to* 2 *(the best possible value) for any possible choice of* n*.*

Generate its truth-table for $n = 4$*,* $n = 5$*, and* $n = 6$*. The truth table of an* (n, n)*-function should be given as a list of* 2^n *integers between* 0 *and* $2^n - 1$*. The inputs and outputs can be seen as* n*-bit integers. For instance, for* $n = 4$*, if we have* $f(0110) = 1110$*, we can write this as* $f(6) = 12$*. The truth table can then be given by the sequence of integers* $f(0), f(1), \ldots, f(2^n - 1)$*. For instance, for* $n = 2$*, the sequence*

$$3, 0, 3, 1$$

corresponds to the function $g(00) = 11$*,* $g(01) = 00$*,* $g(10) = 11$*,* $g(11) = 01$*.*

NB: *When working with finite fields, you can use any primitive polynomial that you like, but you shoud specify which one you are using (since multiplication depends on the choice of the primitive polynomial, and you would get different truth tables for different polynomials.*

Problem 5. ***20%*** *(variant B) The so-called Gold function* $f(x) = x^3$ *in* $\mathbb{F}_{2^n}$ *(that is, as an* (n, n)*-function) is known to have differential uniformity equal to* 2 *(the best possible value) for any possible choice of* n*.*

Prove that x^3 *has differential uniformity* 2 *by the following steps:*

- *consider some input difference* I *and some output difference* O*;*
- *show that the number of solutions* $X \in \mathbb{F}_{2^n}$ *to the equation*

  $$f(X) + f(X + I) = O$$

  is the same as the number of solutions to

  $$f(X) + f(X + 1) = O'$$

  for some O'*;*
- *show that for any choice of* O'*, the above equation cannot have more than* 2 *solutions.*