Criptografie Avansata*

22 noiembrie 2017

1. *Multimi finite.* Pe multimea $\{0, 1, \ldots, 10\}$ se considera un graf orientat definit astfel: pentru orice x si y, muchia orientata $x \to y$ exista daca si numai daca $y = x^2 \bmod 11$. Reprezentati graful orientat si gasiti un ciclu de lungime 4.

2. *Elgamal* in grupul ciclic **aditiv** $(\mathbb{Z}_{1000}, +, 0)$. Deoarece $\gcd(77, 1000) = 1$, $g = 77$ este un generator al acestui grup.

   (a) Pentru generatorul $g = 77$, Alice alege cheia secreta $s = 13$ iar Bob alege cheia efemera $x = 17$. Descrieti numeric calcularea cheii publice de catre Alice, criptarea mesajului clar $m \in \mathbb{Z}_{1000}$ de catre Bob si decriptarea mesajului cifrat de catre Alice.

   (b) Agenta Eva calculeaza $77^{-1} \bmod 1000$ si afla apoi cheia secreta a lui Alice folosind cheia ei publica. Descrieti numeric aceasta procedura.

3. *Elgamal* in inelul $(\mathbb{Z}_{25}, +, \times, 0, 1)$.

   (a) Aratati ca $g = 2$ este un generator pentru grupul **multiplicativ** al unitatilor $(\mathbb{Z}_{25}^{\times}, \times, 1)$, si concludeti ca avem de-a face cu un grup ciclic multiplicativ. *Indicatie: cate elemente are $\mathbb{Z}_{25}^{\times}$, de ce $g = 2 \in \mathbb{Z}_{25}^{\times}$ si ce ordin are $g = 2$ in acest grup?*

   (b) Pentru generatorul $g = 2$, Alice alege cheia secreta $s = 5$ iar Bob alege cheia efemera $x = 6$. Descrieti numeric calcularea cheii publice de catre Alice, criptarea mesajului clar $m \in \mathbb{Z}_{25}$ de catre Bob si decriptarea mesajului cifrat de catre Alice.

4. *RSA* in inelul $(\mathbb{Z}_{26}, +, \times, 0, 1)$.

   (a) Ce perechi $(e, d) =$ (cheie publica, cheie secreta) sunt posibile?

   (b) Pentru cheile publice e gasite mai sus, criptarile RSA mod 26 Enc_e sunt permutari ale multimii $\mathbb{Z}_{26}$. Ce lungimi au ciclurile disjuncte din descompunerile acestor permutari? *Se rezolva fara a calcula explicit permutarile. Ganditi-va la ordinul lui* Enc_e *ca element in grupul* S_{26}.

5. *RSA si criptari bloc.* Alfabetul standard de 26 de litere fara diacritice A_{26} se identifica cu $\mathbb{Z}_{26}$ astfel incat A $= 0, \ldots,$ Z $= 25$. RSA mod 26 se aplica folosind metoda Cypherblock Feedback (CFB) cu cheia publica $e = 5$. Daca vectorul de initializare este $3 \in \mathbb{Z}_{26}$ iar operatia $x \oplus y$ se interpreteaza ca $(x + y) \bmod 26$, sa se cripteze cuvantul SAC.

*Timp de lucru 120 minute.

6. *Corpuri finite de caracteristica* 2. Alfabetul A_{31} este $A_{26} \cup \{\breve{A}, \hat{A}, \hat{I}, \S, \textcyr{Ц}\}$ cu literele suplimentare la sfarsit. Alfabetul A_{31} se identifica cu grupul multiplicativ $\mathbb{F}_{32}^{\times}$, astfel incat A $= 00001 = 1, \ldots,$ Ţ $= 11111 = \omega^4 + \omega^3 + \omega^2 + \omega + 1$. Aritmetica pe $\mathbb{F}_{32} = \mathbb{F}_2[\omega]$ respecta regulile $1 + 1 = 0$ si $\omega^5 + \omega^2 + 1 = 0$. Pentru $k \in \mathbb{F}_{32} \setminus \{0, 1\}$ se considera criptarea $\mathrm{Enc}_k : A_{31} \to A_{31}$ data de $\mathrm{Enc}_k(x) = kx$.

   (a) Criptarile Enc_k definite mai sus sunt permutari ale multimii A_{31}. Ce lungimi au ciclurile disjuncte din descompunerile acestor permutari? *Se rezolva fara a calcula explicit permutarile. Ganditi-va la ciclul care incepe cu* 1.

   (b) Pentru $k = 00011 = \omega + 1$ criptati cuvantul SAC litera cu litera.

   (c) *Facultativ*: Pentru $k = 00011 = \omega + 1$, calculati k^{-1} in corpul $\mathbb{F}_{32}$.

7. *Shamir Secret Sharing.* Cei 5 manageri ai unei companii stabilesc ca oricare 3 dintre ei pot deschide fisierul cu contracte, daca sunt impreuna. Pentru aceasta calculatorul citeste stickurile de memorie ale managerilor prezenti si calculeaza un numar secret $s \in \mathbb{Z}_{13}$. La instalarea sistemului, programul a ales la intamplare un polinom de gradul 2 secret si efemer, $P \in \mathbb{Z}_{13}[X]$ astfel incat $P(0) = s$. Fiecare manager a primit o identitate diferita $\alpha \in \mathbb{Z}_{13}^{\times}$ iar pe stickul lui s-a inregistrat codul de acces $(\alpha, P(\alpha))$, unde $P(\alpha) \in \mathbb{Z}_{13}$. Daca 3 manageri au pe stickurile lor codurile de acces $(3, 9)$, $(5, 1)$ si $(8, 4)$, sa se deduca numarul secret $s \in \mathbb{Z}_{13}$.

8. *RSA in cazul $p = q$.* Fie inelul $(\mathbb{Z}_{p^2}, +, \times, 0, 1)$ cu p prim impar. Atentie: $\varphi(p^2) = p^2 - p$.

   (a) Aratati ca protocolul RSA functioneaza pentru toate mesajele $m \in \mathbb{Z}_{p^2}^{\times} \cup \{0\}$ insa nu functioneaza pentru nici un mesaj m din multimea complementara $p\mathbb{Z}_{p^2} \setminus \{0\} = \{p, 2p, 3p, \ldots, (p-1)p\}$.

   (b) Fie $p = 5$ si cheia publica $e = 13$. Aflati cheia secreta d. Descrieti numeric criptarea de tip RSA a mesajului clar $m = 2$ si decriptarea mesajului cifrat.