Kryptografia, lista 3,

1. Niech f będzie losową funkcją ze zbioru $A = \{1, 2 \ldots, n\}$ w ten sam zbiór.

   - Pokaż, że odwzorowanie takie musi zawierać choć jeden cykl.
   - Jaka jest wartość oczekiwana długości cyklu (podpowiedź: związek z paradoksem urodzinowym) ?
   - Jaki jest związek tych faktów z metodą ρ-Pollarda ?

2. Załóżmy, że w_1 i w_2 są świadkami pierwszości liczby p w teście Fermata. Czy liczba $(w_1 \cdot w_2)^{p^2}$ musi też być świadkiem pierwszości dla liczby p ?

3. Zaproponuj metodę ustalania klucza, która byłaby odporna na atak *man-in-the-middle*, przynajmniej w niektórych scenariuszach. Jeżeli zadnie to wydaje Ci się za trudne, poszukaj opisu protokołu *Interlock* A.Shamira i R.Rivesta.

4. Znamy pewien sekret. Chcemy go „podzielić" pomiędzy naszych przyjaciół Anię, Basię oraz 100 krasnoludków, w taki sposób, aby sekret mógł być odtworzony jedynie przez:

   a) Anię wraz Basią,

   b) 100 krasnoludków przy współpracy Ani lub Basi,

   c) dowolnych dwóch spośród 100 krasnoludków lub wspólnie Anię i Basię,

   d) dowolnych 70 krasnoludków.

   Postaraj się sprawić, żeby każdy ze schematów był możliwie praktyczny.

5. Zaproponuj schemat podpisów cyfrowych, który umożliwiałby weryfikację podpisu wyłącznie przy współpracy wyznaczonej przez podpisującego trzeciej strony.

6. Po co stosujemy standard ISO/IEC 9796 ?

7. W celu redukcji ilości potrzebnych losowych bitów, podczas wykonywania podpisu ElGamala pierwszą połowę bitów parametru losowego zastąpiono wartością funkcji hashującej podpisywanej wiadomości. Czy był to dobry pomysł ?

8. Zaproponuj protokół kryptograficzny, który mógłby działać jak cyfrowe pieniądze.

9. Mówimy nieformalnie, że schemat szyfrowania jest (*semantically secure*), jeżeli na podstawie samego kryptogramu i klucza publicznego nie da się powiedzieć nic o postaci tekstu jawnego. Czy schemat RSA zapewnia tą własność ?

Marek Klonowski