**Шифр Ель-Гамаля**

Для того, щоб зашифрувати деяке число *M*, наприклад 8-байтний ключ, одержувач і відправник виконують наступні дії:

ОДЕРЖУВАЧ:

1. Генерує велике випадкове просте число *p* та ціле число *g* (*g* – генератор, основа степеня, маленьке число) .

2. Обирає закритий ключ – випадкове ціле число *x*: 1 < *x* < *p −* 1 .

3. Обчислює *y = gx* mod *p* .

4. Публікує відкритий ключ (*p; g; y*).

ВІДПРАВНИК:

5. Отримує відкритий ключ (*p; g; y*).

6. Обирає текст для шифрування *M (М – число)*: 1 < *M <* *p −* 1 .

7. Обирає випадкове ціле число *k*: *k –* взаємно простез *p −* 1, *k* < *p −* 1 .

8. Обчислює *a = gk* mod *p* та *b = (yk* *∙ M*) mod *p* .

9. Надсилає одержувачу шифротекст (*a; b*).

ОДЕРЖУВАЧ:

10. Використовуючи свій секретний ключ *x*, розшифровує отриманий шифротекст, користуючись формулою:

*M* ′ *=* (*a* ***p−1− x*** ∙ *b*) mod *p*

***Зауваження 1.***

*a****p − 1 − x*** mod *p =* (*a****p − 1*** ∙ *a* ***− x*** ) mod *p = a****p − 1*** mod *p* ∙ *a* ***− x*** mod *p = a* ***− x*** mod *p*

***3^4 mod 2 = (3\*3\*3\*3) mod 2 = 3^2 mod 2 \* 3^2 mod 2 = 1\*1 =1  
3^4 mod 2 = (3\*3\*3\*3) mod 2 =3 mod 2 \* 3 mod 2 \* 3 mod 2 \* 3 mod 2=1***

***Доведемо, що*** *M* ′ *= M****:***

*M* ′ *=* (*a* ***− x***∙*b*) mod *p = / за п. 10 / =* (*a* ***p−1− x*** ∙*b*) mod *p = / за п.8 / =*

(*g* ***k****(****p−1− x****)*∙ *yk* *∙ M*) mod *p = / за п.3 / =* (*g* ***k****(****p−1− x****)* ∙ *g****kx*** *∙ M*) mod *p =*

= (*g* ***k****(****p−1****) ∙ M*) mod *p = (за малою теоремою Ферма) = М.*

***Зауваження 2:*** число *k* – випадкова величина для кожної сесії, завдяки чому алгоритм Ель-Гамаля отримав назву ***шифру багатозначної заміни***, або ***схеми ймовірнісного шифрування***. При використанні різних значень *k* одержуються різні шифротексти для одного й того самого відкритого тексту *М*, що в цілому підвищує криптостійкість алгоритму.