RSA

Rivest, Shamir, Adleman

1) Выбираем простые p, q: $n = p \cdot q$ $\varphi(n) = (p-1)(q-1)$
2) Выбираем e: $(e, \varphi(n)) = 1$, (e, n) – открытый ключ
3) Вычисляем d: $e \cdot d = 1 \pmod{\varphi(n)}$, (d, n) – закрытый ключ

$X \to X^e \pmod n \rightsquigarrow x^e \to (x^e)^d = x \pmod n$

Диффи – Хеллмана

1) Придумывает a
2) Придумывает b

$a, b \sim 10^{100}$ $p \sim 10^{300}$ $g < 10$

p, g – оба знают

1) Вычисляет $A = g^a \pmod p$
2) Вычисляет $B = g^b \pmod p$

Вычисляет $B^a = (g^b)^a = g^{ba} \pmod p$

Вычисляет $A^b = (g^a)^b = g^{ab} \pmod p$