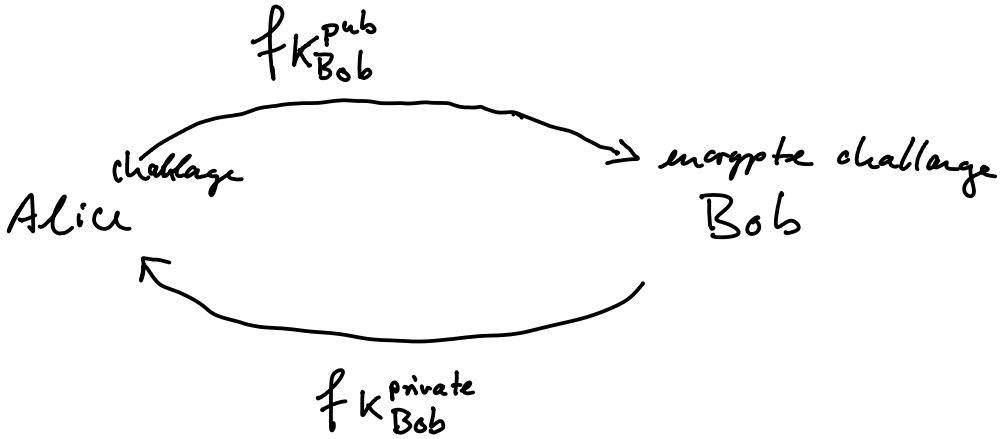
Public Key Cryptosystems

Diffie & Hellmann '76

A public key cryptosystem is a cryptosystem with the property that someone who knows the encyphering key can not (without prohibitively long computation) discover the decyphering key.



This is an example of authentication: Alice wants to make sure she's communicating with Bob, so uses his public key to encrypt a challange and waits for Bob to decipher it and send the challage back. Since Bob (presumably) is the only person knowing the private key, Alice now has confirmed his identity.

The first such system was found by Rivest, Shamir and Adelman in '77.

On the Maths behind it

Definition: Two positive integers are called **coprime** if their gcd is one.

Euler's totient (or phi) function: Given $n \in \mathbb{N}$

$\varphi(n)$ = the number of integer in the range $1, 2, \ldots, n$ that are coprime with n

capital phi: Φ
lower case phi: φ

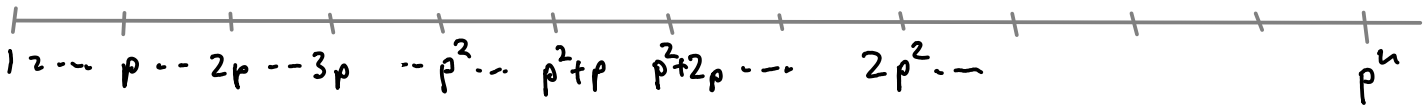
Examples: $\varphi(6) = 2$ $\quad$ 1, ~~2~~, ~~3~~, ~~4~~, 5, ~~6~~

$\varphi(13) = 12$

Proposition: If p is prime, then $\varphi(p) = p - 1$.

Examples: $\varphi(27) = 18 = 3^3 - 3^2$ $\quad$ $27 = 3^3$

$\varphi(32) = 16 = 2^5 - 2^4$ $\quad$ $32 = 2^5$



Proposition: If p is prime, then $\varphi(p^n) = p^n - p^{n-1}$

The only numbers not coprime with p^n are the multiples of p, so $\varphi(n) = p^n - \frac{p^n}{p}$.

Proposition: If n and m are coprime, then

$$\varphi(nm) = \varphi(n)\varphi(m)$$

Example: $\varphi(6) = \varphi(2\cdot 3) = \varphi(2)\varphi(3) = 1\cdot 2 = 2.$

$$\varphi(15) = \varphi(3\cdot 5) = \varphi(3)\varphi(5) = 2\cdot 4 = 8$$

$$\varphi(108) = \varphi(27\cdot 4) = \varphi(3^3)\varphi(2^2) = 18\cdot 2 = 36$$