RSA

- For an attacker to crack the message, he needs to find the values of P and Q using N. This is extremely difficult for large primes.

- Takes more than 70 years if N is 100 digit

- If Alice and Bob use RSA, it'll be difficult to crack their communication

"Factoring as a Service" (https://eprint.iacr.org/2015/1000.pdf), published in 2015, used Amazon EC2 cloud resources to factorize a 512-bit RSA modulus in just four hours for $75. What are the implications for network security?