RSA

- **R**ivest, **S**hamir and **A**delson encryption was the first (1977) publicly known asymmetric encryption algorithm.
- It solved the problem posed by Alice and Bob being unable to meet or securely transfer encryption/decryption keys.
- It also solved the problem of allowing someone to anonymously send an encrypted message to you (Bob).
- This sounds contradictory although it was proposed by Diffie and Hellman and was actually known to British intelligence before RSA was discovered.

The RSA algorithm

- Bob chooses two primes p and q and a number e (for exponent) such that $\gcd(e, (p-1)(q-1)) = 1$.
- Bob creates $n = pq$ and makes n and e public. He definitely does not make p and q public.
- Now Alice (or anyone who wants to anonymously communicate with Bob) takes their message m encoded as a number less than n and computes $m^e \bmod n$ and transmits the outcome to Bob. If their message is long they encode chunks of it as numbers less than n.
- Bob knows a number d (the decrypter) such that $ed \equiv 1 \mod (p-1)(q-1)$ and so he computes $(m^e)^d \bmod n$ and recovers the message m.

Why is RSA so good?

- Because factoring is apparently hard.
- If you are given a number n then it can be written in binary with approximately $b = \log_2(n)$ many bits.
- The naive factoring algorithm tries all numbers up to $\sqrt{n}$ which is a number with about $b/2$ many bits.
- There are about $2^{b/2}$ many numbers with $b/2$ many bits and so the naive algorithm takes exponentially long in the length of the number in order to factor it.
- There are better algorithms but they still do not factor quickly.
- The best RSA challenge that has been passed was the factorization of a 768 bit number. The hardest unsolved RSA challenge is 2048 bits long.

RSA-2048

2519590847565789349402718324004839857142928212620 40
3202777713783604366202070759555626401852588078440 69
1829064124951508218929855914917618450280848912007 28
4499268739280728777673597141834727026189637501497 18
2469116507761337985909570009733045974880842840179 74
2910064245869181719511874612151517265463228221686 99
8754918242243363725908514186546204357679842338718 47
7444792073993423658482382428119816381501067481045 16
6037730605620161967625613384414360383390441495263 44
3219011465754445417842402092461651572335077870774 98
1712577246796292638635637328991215483143816789988 50
4044536402352738195137863656439121201039712282212 07
20357

All you need to know about primes

- RSA needs lots of primes to stay ahead of technology.
- Recall that Euclid proved to us that there are infinitely many primes.
- In fact we know that primes are not that rare. Let $\pi(N)$ be the number of primes $\leq N$. The following theorem was proved by Hadamard and de la Valleé in the 19^{th} century.

Theorem (Prime Number Theorem)

$$\pi(N) \sim \frac{N}{\ln(N)}.$$

That is,

$$\lim_{N \to \infty} \frac{\pi(N)\ln(N)}{N} = 1.$$

Back to modular arithmetic

- $a \equiv b \mod n$ if n divides $a - b$.
- For each n, this is an equivalence relation on the integers.
- As with 26, addition and multiplication is well-defined for integers mod n.
- As before, we get a ring (all the usual rules of arithmetic work) on the integers mod n.
- The set of equivalence classes is written Z/nZ and when one talks about arithmetic operations, one is talking about addition and multiplication of classes.