p1 q7
PR

Discrete mathematics 2002

Long question A

for d

State Fermat's Little Theorem and derive the Diffie-Hellman key exchange protocol. [6 marks]

The protocol requires repeated multiplication (mod p), for some prime p, to achieve exponentiation. On most computers this requires division by p after each multiplication to calculate the remainder, which can be slow. *Montgommery multiplication* avoids the division as follows:

Given an odd prime p, let B be a power of 2 with $B > p$. Define $m(x) \equiv xB \pmod{p}$. Prove that:

- $m: \mathbb{Z}_p \to \mathbb{Z}_p$ is a bijection.
- $m(x \times y) = m^{-1}(m(x) \times m(y))$. [6 marks]

Given $u < pB$, let $v \equiv -up^{-1} \pmod{B}$ and $x = (u + vp) \div B$. If $x \geq p$, then subtract p from x. Prove that:

- x is an integer.
- $x \equiv uB^{-1} \pmod{p}$.
- $x < p$. [6 marks]

Deduce that $x = m^{-1}(u)$, ~~and observe~~ observing that its calculation only involves division by B. [2 marks]

Answer

Fermat:

Given a prime p and a value a which does not have p as a factor, then $a^{p-1} \equiv 1 \pmod{p}$. [2]

Diffie-Hellman:

Choose a large prime modulus, p. Pick e with $(e, p-1) = 1$ and find d such that $de \equiv 1 \pmod{p-1}$ so $de = 1 + (p-1)t$ for some t.

Observe $(a^e)^d = a^{ed} = a^{1+(p-1)t} = a(a^{p-1})^t \equiv a1^t \pmod{p} = a$ by Fermat. [2]

- Alice chooses p and the value e and sends p and the message a^e to Bob.
- Bob picks another value f with inverse g and sends $(a^e)^f$ back to Alice.
- Alice works out $((a^e)^f)^d = ((a^e)^d)^f = a^f$ and sends it back to Bob.
- Bob now works out $(a^f)^g$ to recover a. [2]

Montgommery:

B is a power of 2 and p is odd, so they are co-prime and B has a reciprocal (mod p). Therefore m has inverse $m^{-1}(u) \equiv uB^{-1} \pmod{p}$. [4]

$m(x \times y) \equiv xyB \pmod{p} = xB\, yB\, B^{-1} \pmod{p} \equiv m^{-1}(m(x) \times m(y))$. [2]

$u + vp \equiv u - up^{-1}p \pmod{B}$ $vp \equiv u - u = 0$, so $u + vp$ is a multiple of B. [2]

$x = (u + vp)\, B^{-1} \equiv uB^{-1} \pmod{p}$. [2]

$u < pB$ and $v < B$ so $u + vp < 2pB$ and $x < 2p$. But we then subtract p from x if $x \geq p$, leaving $x < p$. [2]

$x \equiv uB^{-1} \pmod{p}$ and $x < p$ so $x = m^{-1}(u)$. [2]