Answers to Chapter 8 questions

Activity 8.1

a

Stage	Sender	Recipient
1	the sender uses an encryption algorithm (see later) and chooses a value – e.g. X = 3 (this is kept secret)	the recipient uses the same algorithm and also chooses a value – e.g. Y = 5 (this is also kept secret)
2	this value of X is put into a simple algorithm: 7^3 (MOD 11) (MOD gives the remainder when dividing a number by 11) this gives: 7^3 (MOD 11) = 343 (MOD 11) which gives the value: 2 (i.e. 31 remainder 2)	the value of Y is put into the same algorithm: 7^5 (MOD 11) (MOD gives the remainder when dividing a number by 11) this gives: 7^5 (MOD 11) = 16807 (MOD 11) which gives the value: 10 (i.e. 1527 remainder 10)
3	the sender now sends the value just calculated (i.e. 2) to the recipient	the recipient now sends the value just calculated (i.e. 10) to the sender
4	this new value is put into the same algorithm – the new value replaces "7": 10^X (MOD 11) this gives: 10^3 (MOD 11) = 1000 (MOD 11) which gives the value: 10 (i.e. 90 remainder 10)	this new value is put into the same algorithm the new value replaces "7": 2^Y (MOD 11) this gives: 2^5 (MOD 11) = 32 (MOD 11) which gives the value: 10 (i.e. 2 remainder 10)

b

Stage	Sender	Recipient
1	the sender uses an encryption algorithm (see later) and chooses a value – e.g. X = 7 (this is kept secret)	the recipient uses the same algorithm and also chooses a value – e.g. Y = 6 (this is also kept secret)
2	this value of X is put into a simple algorithm: 7^7 (MOD 11) (MOD gives the remainder when dividing a number by 11) this gives: 7^7 (MOD 11) = 823543 (MOD 11) which gives the value: 6 (i.e. 74867 remainder 6)	the value of Y is put into the same algorithm: 7^Y (MOD 11) (MOD gives the remainder when dividing a number by 11) this gives: 7^6 (MOD 11) = 117649 (MOD 11) which gives the value: 4 (i.e. 10695 remainder 4)
3	the sender now sends the value just calculated (i.e. 6) to the recipient	the recipient now sends the value just calculated (i.e. 4) to the sender
4	this new value is put into the same algorithm – the new value replaces "7": 4^X (MOD 11) this gives: 4^7 (MOD 11) = 16384 (MOD 11) which gives the value: 5 (i.e. 1489 remainder 5)	this new value is put into the same algorithm the new value replaces "7": 6^Y (MOD 11) this gives: 6^6 (MOD 11) = 46656 (MOD 11) which gives the value: 5 (i.e. 4241 remainder 5)