AES (Advanced Encryption Standard)

- a block cipher that operates on bytes and encrypts 128-bit, 168-bit, 192-bit, 224-bit, or 256-bit data blocks
    - using a 128-bit, 192-bit, or 256-bit key
- the standard AES in practice is AES-128, where both the data block and key are 128 bits in size
- uses several rounds of encryption
    - the entire block of data is encrypted in each of the rounds
- depending on the size of the key used, the number of rounds performed varies
    - for a 128-bit key, there are 10 rounds
    - for a 192-bit key, there are 12 rounds
    - for a 256-bit key, there are 14 rounds
- each round has a separate sub-key that is based on the Rijndael key schedule
    - a mathematical function that expands a key into a number of separate round keys

- background story
    - at the time, DES (Data Encryption Standard) had been broken
        - so there was a desperate need for AES
    - NIST announced an AES competition and issued a call for algorithm submissions
        - 15 were submitted
        - 5 made it to the finals
        - finalists?
            - Ron Rivest, IBM, etc
        - Rijndael, designed by two young Belgian cryptographers, won
            - named after Joan Daeman and Vincent Rijmen
            - later became AES

    - today, AES is the most-widely used encryption algorithm
    - NSA allows AES to encrypt top secret documents (if a 192-bit or larger key is used)

- AES working mechanism
    - each round (except the last one) has four layers:
        1. byte substitution
        2. row shift
        3. column mix
        4. key addition
        - (the last round does not have the column mix layer)

    - to begin, the data is arranged in a 4x4 matrix
        - e.g., “Sky is falling”:

	0	1	2	3
0	S	i	a	n
1	k	s	l	g
2	y		l	#
3		f	i	#

- note that the blank cells contain a space
- the final two # symbols are padded characters
- padding?

when the data block is not 16 bytes long, it is padded by appending some values at the end
the most basic form of padding is to append 0’s at the end (we add #'s)

1. byte substitution (i.e., confusion)
16 bytes of input data (=128 bits)
each byte is substituted using a substitution box (S-box)
an S-box is just a constant matrix that substitutes bits for other bits
it is defined to be strong against numeric attacks (which makes the cipher stronger)
2. row shift (i.e., diffusion at an algorithmic level)
each row in the matrix above is shifted to the left by 0, 1, 2, and 3 respectively
the output for the matrix above after the row shift is:

	0	1	2	3
0	S	i	a	n
1	s	l	g	k
2	l	#	y	
3	#		f	i

3. column mix (i.e., diffusion)
diffuse the data so that even a single change in an input changes everything on the output
a different matrix is used to perform polynomial multiplication on the row shift matrix above:

	0	1	2	3
0	2	3	1	1
1	1	2	3	1
2	1	1	2	3
3	3	1	1	2

note: each of the letters on the row shift matrix corresponds to some binary value
binary values are multiplied with the above matrix
a dot product
4. key addition
the output obtained after matrix polynomial multiplication is XOR’d with this round's sub-key
recall the Rijndael key schedule above for generating round keys

in general, for *n* rounds, to get the ciphertext:
the four layers are performed in all rounds 1 to *n*-1
all but the column mix layer is performed in the final (*n*-th) round

security of AES
depends on confusion and diffusion
polynomial matrix multiplication diffuses the input at a great level