Quantum Computers compromise symmetric key cryptography because it essentially depends on two large prime number factors forming a large number, with one factor each constituting the private key and the public key. If an attacker can factorize the large number, they then have the keys.

Peter Shor's algorithm for quantum factorization transforms the factorization problem into a problem of finding the period of a function. Then Quantum Computers are orders of magnitude better at this period finding problem than classical computers.

So, what is Shor's algorithm?

Shor's algorithm reduces "the factorization of N" problem into a problem of "finding the period P of the function f(x)=R^x mod N, where R is a random number less than N which is not already a factor of N".

Example, factorizing 30 using Shor's Algorithm

Step 1: pick a random number less than 30. Say 7
Step 2: verify it is not already a factor. GCD(7,30) is 1 or 30 mod 7 is 2 which is > 0
Step 3: define a function f(x) = 7^x mod 30

X	F(x)	X	F(x)	X	F(x)
1	7	2	19	3	13
4	1	5	7	6	19
7	13	8	1	.. and so on	

As we can see, period is 4.

Step 4: factors are **GCD(R^(P/2)+1, N)** and **GCD(R^(P/2)-1, N)**

7^(4/2) = 49. Plus 1 = 5 and Minus 1 = 48
GCD(48,30)=6 (Greatest Common Divisor)
GCD(50,30)=10
So, the factors are 6 and 10.
We can now do this recursively to find prime factors.

Why are Quantum Computers better at finding period?

In very simplified and not necessarily most accurate terms, we can explain this something like: A Quantum Bit or Qubit is a superposition state – it simultaneously holds all values b/w 0 and 1. So if x is represented in Qubits, then doing f(x) on this set of qubits representing x gives us all the values of f(x) at the same time. Doing a quantum Fourier transform on this results in a probability wavefunction that has an interference pattern which tells us the period of f(x). So step 3 is super easy with a Quantum Computer but super hard with a classical computer.

Is Cryptography really at risk?

Current quantum computers have the order of 100 qubits and can maintain superposition for the order of microseconds. On the other hand, to break 2048 key RSA algorithm, we need 20 million qubits at superposition for 8 hours. So while theoretically cryptography is at risk, realistically that day is very far away.