How Quantum Computing pose a threat for the standard encryption methods?

Any system using public-key encryption will be vulnerable to an attack by a quantum computer and systems using certain types of AES, such as AES-128, must double their current key length to be remain secure. This would drive the time required to break AES encryption up to 2.29\*10^32 years

Describe the two classes of solutions available for quantum-safe communication methods.

Extended Validation (EV):

Extended Validation (EV) SSL certificates provide the highest level of trust and are the industry standard for business websites.To receive one, website owners must meet the authentication requirements for an OV SSL but also go through a stricter vetting process performed by a human specialist.

Organization Validation (OV):

Organization Validation (OV) SSL certificates are a step up from DV. To receive one, an organization must prove it owns the domain it wishes to secure and confirm that it is a legally registered business. These can only be issued to a registered organization and not individuals, making them more suitable for public-facing websites.

Domain Validation (DV):

Domain Validation (DV) SSL certificates provide the quickest, easiest, and most cost-effective way to receive industry-standard encryption. This validation type requires proof of ownership for the secured domain and is typically issued within minutes

Describe the “public-key” cryptography and the RSA protocol.

In a public-key cryptosystem, the encryption key is public and distinct from the decryption key, which is kept secret (private). An RSA user creates and publishes a public key based on two large prime numbers, along with an auxiliary value. The prime numbers are kept secret.

List the advantages and challenges of Quantum Key Distribution.

QKD solves the same problem as public-key cryptography: it allows two parties (Alice and Bob) to establish a secret key between them. The key can then be used with symmetric- key cryptography to communicate securely. In QKD, Alice and Bob communicate using single particles of light, called photons.

Quantum key distribution promises unconditional security in data communication and is currently being deployed in commercial applications. Nonetheless, before QKD can be widely adopted, it faces a number of important challenges such as secret key rate, distance, size, cost and practical security.

What practical challenges you foresee to implement quantum-safe communications in Healthcare?

IBM expects quantum computing to transform the healthcare sector from as early as 2030. From speeding up diagnoses to personalising medicine and reducing costs, the algorithms used by quantum technology can be used to accelerate the drive for efficiency in medical services across the world.

I belive the Humanity aspect will be missing in alot of the Doctors visits.