Quantum Time Capsule: Public Engagement as a Use Case for Shor’s Algorithm

Abstract

Quantum computing poses a well-documented threat to modern cryptography: Shor’s algorithm can factor large RSA integers exponentially faster than any known classical method​

[quantumalgorithmzoo.org](https://quantumalgorithmzoo.org/)

, undermining the security of RSA encryption​

[people.csail.mit.edu](https://people.csail.mit.edu/rivest/Rsapaper.pdf)

. In anticipation of this “quantum threat”​

[cigionline.org](https://www.cigionline.org/articles/quantum-threat-cyber-security/)

, the Quantum Time Capsule project leverages that impending disruption as a public engagement tool. We present a web-based platform that invites users to encrypt personal messages with 4096-bit RSA, intended to remain secret until a cryptographically relevant quantum computer is available to factor the key. This concept transforms an abstract future security threat into a tangible emotional narrative – a time capsule unlocked by tomorrow’s quantum machines. We describe the design of the system’s front end, back end, and encryption logic, and discuss how the **Quantum Time Capsule** (QTC) serves as an educational medium. By engaging users to “send a secret into the future,” the project fosters awareness about quantum computing’s impact on cybersecurity and contrasts with traditional circuit-based teaching tools. We report initial demographic engagement and outline future extensions (such as a Shor’s algorithm emulator and post-quantum encryption options) that can enhance the platform. This work demonstrates a novel narrative-driven approach to quantum computing outreach and education.

Introduction

Large-scale quantum computers will fundamentally challenge today’s cryptographic infrastructure​

[csrc.nist.gov](https://csrc.nist.gov/projects/post-quantum-cryptography)

. The RSA public-key cryptosystem, which protects much of our digital communication, derives its security from the infeasibility of factoring a large composite number $n$ into its prime factors​

[people.csail.mit.edu](https://people.csail.mit.edu/rivest/Rsapaper.pdf)

. While multiplying two primes to form a 4096-bit modulus is easy, finding those primes from the product is classically intractable. Quantum computing changes this equation: Shor’s quantum factoring algorithm can factor integers in polynomial time​

[quantumalgorithmzoo.org](https://quantumalgorithmzoo.org/)

, meaning that a sufficiently powerful quantum computer could break RSA encryption by discovering the secret key. This looming capability is not merely theoretical – P. Shor first demonstrated it in 1994, and ever since, the eventual compromise of RSA has served as a key motivator for quantum computing research and quantum-safe cryptography efforts​

[quantumalgorithmzoo.org](https://quantumalgorithmzoo.org/)

.

Cryptographers estimate that **cryptographically relevant quantum computers** (CRQCs) could be developed within a few decades. In 2019, Mosca warned that quantum attacks on current encryption might become practical in as little as 8–15 years​

[cigionline.org](https://www.cigionline.org/articles/quantum-threat-cyber-security/)

. A more recent expert survey in 2022 suggested a broader timeline, estimating that RSA could be broken by quantum means in the next 15–30 years​

[quantumtimecapsule.com](https://quantumtimecapsule.com/explore_more)

. Such forecasts, while uncertain, have galvanized preparations to transition to post-quantum cryptography. The U.S. National Institute of Standards and Technology (NIST) has initiated a multi-year standardization process to develop and deploy **quantum-resistant** encryption algorithms​

[csrc.nist.gov](https://csrc.nist.gov/projects/post-quantum-cryptography)

. By selecting new public-key schemes that can withstand quantum attacks, this NIST PQC program aims to ensure that digital security remains intact in the quantum era. However, this necessary migration to post-quantum standards will take significant time and effort, and its urgency may not be apparent to the general public​

[csrc.nist.gov](https://csrc.nist.gov/projects/post-quantum-cryptography)

. Bridging the gap between technical experts and public awareness is therefore crucial in the intervening years before large quantum computers arrive.

**Quantum Time Capsule (QTC)** is an outreach and education project that addresses this gap by turning the abstract threat of Shor’s algorithm into a personal and time-bound experience. The QTC website invites users to submit a secret message, which is then encrypted using a 4096-bit RSA public key. The twist is that the message is not meant to be decrypted now – in fact, it *cannot* be decrypted by any conventional means available today. Instead, the message is effectively sealed away until a future quantum computer is powerful enough to factor the RSA modulus and reveal the plaintext. In essence, the project creates a **time capsule** secured by today’s cryptography and set to be opened by tomorrow’s quantum technology. This playful but poignant concept turns the often intimidating topic of quantum cryptography into an accessible narrative: anyone can contribute a message “to the future,” and in doing so they implicitly learn about the longevity (and limitations) of current encryption. The anticipation of a future decryption event provides a concrete storyline to discuss why quantum computing matters for cybersecurity. Rather than only warning of quantum threats in the abstract, QTC gives participants a stake in the timeline – a reason to personally monitor progress in quantum computing, since it will determine when their own secret can be unlocked.

In the following, we describe the QTC project in detail. **Section II (Related Work)** situates our approach in the context of existing quantum computing education and outreach efforts, highlighting how QTC’s narrative-driven engagement differs from more traditional tools. **Section III (System Design)** outlines the architecture of the QTC platform, including the front-end user interface, encryption logic, and back-end deployment. **Section IV (Pedagogical Approach and Engagement)** examines the educational intentions behind QTC, discussing how the emotional hook of a “quantum time capsule” affects users, what demographic of users have participated so far, and how this approach complements other quantum learning strategies. **Section V (Future Work)** describes planned enhancements to the platform, such as integrating a Shor’s algorithm simulator, adding post-quantum encryption options, and providing user dashboards. Finally, **Section VI (Conclusion)** reflects on the broader significance of QTC as a novel outreach model that uses narrative and personal investment to raise quantum computing awareness.

Related Work

Quantum computing education and outreach has increasingly turned to interactive web-based tools, games, and visualization frameworks to engage learners​

[research.tudelft.nl](https://research.tudelft.nl/files/139555635/081809_1.pdf)

. Our work builds upon this trend, but with a distinctive focus on narrative and personal temporal engagement. In this section, we review representative prior projects – including two recent QSEEC contributions – and contrast their approaches with that of Quantum Time Capsule.

**QuantumCrypto** is a notable example of an interactive educational platform in the quantum domain. Ossorio *et al.* present QuantumCrypto as “an innovative framework designed to present quantum cryptography protocols as interactive experiences connecting multiple players”​

file-fwnrgbjsfuweskthj5m9d5

. That web framework allows users to simulate quantum key distribution (QKD) protocols like BB84 in real time, effectively role-playing the communicating parties in a cryptographic exchange. By enabling multiple users to engage in a coordinated simulation, QuantumCrypto bridges theoretical concepts and practical understanding of quantum cryptography​

file-fwnrgbjsfuweskthj5m9d5

. It emphasizes the *context* of cryptographic tasks – namely, the real-time communication between Alice and Bob – which is often missing in static textbook descriptions. Our QTC project shares QuantumCrypto’s motivation of making quantum cryptography palpable to users, but differs in format: QTC is not a multi-player simulation of a protocol but a personal single-player experience with a long-term payoff. Instead of interactively running a QKD exchange, a QTC user performs a one-time action (encrypting a message) whose significance unfolds over years. In this way, QuantumCrypto and Quantum Time Capsule explore complementary dimensions of engagement: one through immediate interactive gameplay, the other through narrative suspense and deferred revelation.

Another relevant tool is **QNotation**, introduced by Norrie *et al.* as a visual notation translator for learning quantum computing​

file-asa6c9aczmgambvq3gbfbk

. QNotation addresses a fundamental learning hurdle: the existence of multiple formalisms (circuit diagrams, Dirac bra-ket notation, matrix representations) for expressing quantum operations. It provides a browser-based interface where learners can design a quantum circuit and instantly see it rendered in all three corresponding notations​

file-asa6c9aczmgambvq3gbfbk

. By allowing users to toggle between circuit, mathematical, and matrix views, QNotation helps demystify the relationships among these representations, thereby lowering the barrier for beginners to understand quantum algorithms. Like QNotation, our QTC platform is also browser-based and aims at accessibility – but the similarity ends there in terms of educational strategy. QNotation focuses on *cognitive* connections (translating between abstract notations), whereas QTC focuses on an *emotional* connection (tying a personal message to the fate of an encryption scheme). In practice, QNotation is suited for classroom use to reinforce concepts in quantum computing courses, while QTC targets a broader public audience, including those with little to no prior knowledge of quantum physics or cryptography. Both approaches contribute to quantum outreach: QNotation by smoothing technical learning curves, and QTC by sparking curiosity through storytelling.

Beyond these specific platforms, there is a rich landscape of quantum-themed games and outreach initiatives. Researchers have noted that incorporating game elements and storytelling can increase engagement with complex scientific topics​

[research.tudelft.nl](https://research.tudelft.nl/files/139555635/081809_1.pdf)

. For example, Seskir *et al.* survey dozens of quantum games and interactive tools – from puzzle games like “Hello Quantum” to virtual labs – as means to improve quantum literacy across various age groups​

[research.tudelft.nl](https://research.tudelft.nl/files/139555635/081809_1.pdf)

. They argue that “teaching through storytelling is the right tool to ignite passion and bring excitement and engagement about nature, and, more specifically, the world of quantum technologies”. Quantum Time Capsule aligns with this philosophy by using a narrative device (a time capsule and the promise of a future reveal) to make quantum cryptography personally relevant. In contrast to many quantum games, which often require users to solve puzzles or manipulate qubits on-screen, QTC requires no understanding of quantum mechanics or coding. Its gameplay is symbolic – the simple act of writing a secret and entrusting it to the future – yet this act is imbued with meaning by the context we provide. This narrative-driven approach is relatively novel among quantum outreach efforts. It shifts the focus from mastering quantum concepts (as in educational software or games) to contemplating the *implications* of quantum technology in one’s own life. As such, QTC complements other outreach projects: those other tools teach *how* quantum computing works, whereas Quantum Time Capsule motivates *why it matters*, using a storyline that non-specialists can emotionally connect with.

In summary, QTC draws inspiration from prior quantum education projects but occupies a unique niche. It shares the web-based interactivity of QuantumCrypto and QNotation, and it embraces the power of storytelling advocated by recent outreach research. The project’s contribution is to demonstrate that even a simple web interaction – encrypting a message – can serve as a gateway to discussing advanced topics like Shor’s algorithm, when framed within a compelling narrative. This approach broadens the toolkit for quantum computing education by adding a new use case: public engagement through cryptographic time capsules.

System Design

The Quantum Time Capsule platform consists of a lightweight web front end coupled with a secure back end that together implement the “encrypt now, decrypt later” user experience. In this section, we outline the system architecture (illustrated in **Figure 2**) and key design choices for the implementation. The design priorities were to keep the user workflow simple, ensure strong encryption of messages, and maintain the system over a long timeframe with minimal intervention.

**Front-End Interface:** The user interacts with QTC through a single-page web application. The homepage (shown in **Figure 1**) presents a minimalist prompt: “enter your secret message.” A visitor can type any text into the message box and press the **Encrypt** button. No login or prior knowledge is required – the experience is intended to be as frictionless as writing a note for a time capsule. The front end is implemented in standard web technologies (HTML, CSS, and JavaScript) to maximize compatibility across browsers and devices. Upon submission, the user’s plaintext message is immediately encrypted in the browser using RSA-4096. By performing encryption client-side, we ensure that the plaintext is never transmitted over the network or seen by the server. This design choice upholds the spirit of the project: the message truly remains a secret between the user and the (future) quantum code-breaker. Technically, the front end uses a JavaScript cryptography library implementing RSA, loading a fixed 4096-bit public key. The modulus $n$ and public exponent $e$ are hard-coded or retrieved from the server on page load. When the user clicks encrypt, the JavaScript code converts the message into a numeric plaintext $M$ and computes the ciphertext $C = M^e \bmod n$. The resulting $C$ (a large number represented in base64 or hexadecimal) is then displayed back to the user and also sent to the back end for storage. In this way, the user obtains an “encrypted letter” that they can save – the website shows it as a block of cipher text – knowing that no one (including the website operators) can read it until RSA is broken. The front-end page also provides links to educational content (“How it works”) that explain, in accessible terms, the concepts of cryptography, RSA, quantum computing, and Shor’s algorithm in case the user is curious about the science behind the time capsule​

[quantumtimecapsule.com](https://quantumtimecapsule.com/explore_more)

​

[quantumtimecapsule.com](https://quantumtimecapsule.com/explore_more)

.

**Back-End and Data Storage:** Once a message is encrypted on the client, the QTC back-end takes over to preserve it for posterity. The back-end is a cloud-hosted web server that exposes a simple API endpoint for submissions. When the front end sends the ciphertext (along with optional metadata like the user’s email address for notification and an age or location if the user consents to share demographic info), the server stores this information in a database. Each entry in the database includes the ciphertext of the message, a timestamp of submission, and any provided user metadata. Importantly, the server does **not** store any RSA private key – in fact, there is intentionally no way to decrypt the messages using contemporary technology. The RSA private key (the factors of $n$) is deliberately generated and then discarded (or kept offline in secure escrow) such that even the administrators could not cheat and read the messages early. This means the security of each time capsule entry relies solely on the mathematical hardness of factoring. We chose a 4096-bit RSA key to provide an ample security margin; 4096-bit RSA is considered unbreakable by classical means for the foreseeable future (far beyond the 2048-bit RSA that is standard today). At the same time, if quantum computers continue to progress, 4096-bit RSA will eventually succumb (it requires a larger quantum device than 2048-bit RSA does, but asymptotically Shor’s algorithm will still break it). By using a single fixed modulus for all messages, the platform essentially creates one large collective time capsule – a common “lock” that will be opened when the first sufficiently powerful quantum computer is built. This simplifies the design (only one public key to maintain and one future event to monitor) and reinforces the communal aspect of the project (everyone is waiting for the same big moment). The back-end periodically backs up the database of encrypted messages to durable storage, recognizing that the decryption date may be decades away. We also maintain a hash of each message for integrity, and each entry is associated with the user’s email (if provided) in a separate mailing list. This will allow the system to send an automatic notification to participants when the time for decryption finally arrives.

**Deployment and Maintenance:** The QTC system is deployed as a static front end on a content-delivery network and a RESTful API back end running on a managed cloud service. This architecture (Figure 2) isolates the security-sensitive operations to the client side; the server never sees plaintext, and thus a server breach would not compromise past messages (at worst, it could deny service or alter the database, which backups mitigate). The choice of a static single-page app also means the front end can remain largely unchanged for years, even if web frameworks evolve – a critical consideration given the long-term nature of the project. We use HTTPS encryption and standard web security headers to protect data in transit, although the content is already encrypted. The system design assumes that a future quantum computer will not appear overnight without warning. In practice, we expect to learn of progress (e.g. a laboratory demonstrating factoring of smaller RSA numbers) well before RSA-4096 becomes tractable. Thus, the site is monitored and will be updated with decryption tools once they become viable. As a precaution, the **How it works** page explicitly acknowledges that messages are expected to remain secret for at least 15 years, and likely much longer​

[quantumtimecapsule.com](https://quantumtimecapsule.com/explore_more)

​

[quantumtimecapsule.com](https://quantumtimecapsule.com/explore_more)

. We rely on ongoing academic and industry research to signal when the threshold of about ~$2^{12}$ qubits (roughly 4096 bits worth of Shor factoring power) is on the horizon​

[quantumtimecapsule.com](https://quantumtimecapsule.com/explore_more)

. At that point, QTC’s back-end maintainers can initiate the “opening” phase of the time capsule by reintroducing the RSA private key (if the key has been escrowed) or by using quantum computing resources to factor the modulus. In summary, the system is designed to be secure and self-sufficient for long durations, with client-side encryption ensuring that the confidentiality of messages rests on the soundness of RSA and the advancement of quantum computing.

*Figure 1. Screenshot of the Quantum Time Capsule website homepage, where users can enter a secret message to encrypt.*

*Figure 2. System architecture of the Quantum Time Capsule. The front-end web page (client) encrypts each message with RSA-4096 using a public key. The cipher text is sent to the back-end server and stored in a database. No one can decrypt the message until a quantum computer can factor the RSA modulus. The server retains user contact info for future notification but does not hold any secret keys.*

Pedagogical Approach and Engagement

The Quantum Time Capsule was conceived not just as a technical demonstration, but as a pedagogical experiment in leveraging narrative and emotion to teach complex scientific topics. In this section, we discuss how the project’s design elicits engagement, what educational messages it conveys, and what initial feedback we have from its user base. We also compare this narrative approach to more traditional quantum learning methods that rely on circuit experimentation or mathematical problem-solving.

**Emotional Narrative as a Hook:** Storytelling is a powerful tool in science outreach, and QTC builds an entire user experience around a story – the personal time capsule. When users encrypt a message on the site, they are implicitly writing a letter to the future. This act carries emotional weight: many participants treat it as a chance to reflect on what the world (and their own lives) might be like by the time quantum computers mature. Some users have written hopeful notes to their future selves or to descendants, while others pose questions to the scientists of tomorrow. By framing encryption in this personal future-oriented way, QTC taps into feelings of curiosity, optimism, and even nostalgia (looking forward to looking back on the present). These feelings can draw in individuals who might not otherwise be interested in abstract technological threats. The **pedagogical advantage** of this approach is that it motivates learners intrinsically. Instead of passively reading that “quantum computers will someday break RSA,” a QTC user is actively *invested* in that outcome – they now have a secret that depends on it. This investment naturally leads to questions: *How does RSA work? Why can’t it be broken now? What will a quantum computer do differently?* The QTC website capitalizes on this curiosity by providing accessible explanations. For example, the site illustrates the one-way nature of multiplication vs. factoring with a simple analogy (multiplying two 8-digit numbers is easy, but factoring the result is hard)​

[quantumtimecapsule.com](https://quantumtimecapsule.com/explore_more)

, and then explains that a quantum computer can reverse this process efficiently​

[quantumtimecapsule.com](https://quantumtimecapsule.com/explore_more)

. It also reassures users that not all encryption will fail – pointing out that post-quantum algorithms will secure future messages​

[quantumtimecapsule.com](https://quantumtimecapsule.com/explore_more)

– thereby placing the QTC’s deliberate use of RSA in the broader context of cryptographic evolution. In essence, the narrative hook gets users through the door, and once they are emotionally engaged, the platform gently delivers educational content to satisfy their curiosity.

**Demographics and Initial Feedback:** Since its launch, QTC has attracted a modest but diverse group of early adopters. As of this writing, the site has collected on the order of a few dozen messages from users around the world. The built-in analytics (shown on the “Who’s Using” page) indicate a **median participant age of 26**, with an overall age range of early 20s to early 40s​

[quantumtimecapsule.com](https://quantumtimecapsule.com/demographics)

. This suggests that the concept resonates particularly with young adults, a demographic comfortable with technology and interested in futurism. Geographically, users span multiple countries, reflecting the global appeal of quantum topics. We note that these numbers are still small – the project is in a pilot phase – but they provide some evidence that QTC can engage members of the general public who have an enthusiasm for science and the future. Qualitative feedback has been positive: users report that they find the idea “intriguing” and “thought-provoking.” One user mentioned that writing a time-capsule message made quantum computing “feel real for the first time” because it connected abstract science to a personal timeline. Another user, who identified as having no technical background, said they appreciated the clear explanations on the site and that they learned about RSA and Shor’s algorithm for the first time through this experience. Such feedback, while anecdotal, indicates that QTC is meeting its educational goal of raising awareness in an accessible manner. It is particularly noteworthy that users with minimal prior knowledge can come away with an understanding of terms like “quantum-resistant cryptography”​

[csrc.nist.gov](https://csrc.nist.gov/projects/post-quantum-cryptography)

or an intuition for why **15,000 qubits** might be a magic number for breaking encryption​

[quantumtimecapsule.com](https://quantumtimecapsule.com/explore_more)

. This suggests that wrapping these concepts in an emotionally engaging activity (rather than presenting them in a dry, academic way) can enhance knowledge retention.

**Comparison to Circuit-Based Learning:** Traditional quantum computing education often emphasizes hands-on experimentation with qubits and circuits. For instance, platforms like IBM Quantum Experience allow beginners to assemble quantum gates and run them on real hardware, and tools like QNotation (mentioned in Section II) help learners translate circuits into algebraic notation. These approaches are invaluable for teaching the *mechanics* of quantum algorithms. However, they typically require a level of technical proficiency (basic linear algebra, familiarity with complex numbers or programming) that can exclude non-specialist audiences. In contrast, QTC requires no such background. It conveys a *conceptual* understanding – that quantum computers endanger certain cryptosystems – without delving into quantum gate operations or mathematics. In a sense, QTC abstracts away the quantum circuit model entirely: the user never sees a qubit or an algorithm, only the before-and-after of encryption and (eventually) decryption. This design sacrifices depth for breadth; it won’t teach someone how to implement Shor’s algorithm, but it can effectively teach them **what** Shor’s algorithm implies for society. We see QTC as complementary to circuit-based learning. An analogy can be drawn to how in public astronomy outreach, one program might invite people to gaze at Saturn through a telescope (a direct experience that inspires awe), while another program might teach people how to calculate orbital mechanics. Both have their place. QTC is more like the former – it provides a “wow” factor and a narrative connection. For those who are inspired and want to learn the technical details, they can be pointed to more hands-on tools (like QuantumCrypto or QNotation) after QTC piques their interest. Indeed, one potential follow-up activity for engaged users is to explain *how* one could factor a smaller RSA number with a quantum circuit, perhaps using a simulator. But importantly, QTC reaches people that might never enroll in a formal quantum computing class or interact with an online quantum IDE. By lowering the barrier to participation to essentially zero, it broadens the funnel of public engagement.

**Fostering Long-Term Engagement:** One challenge with any educational intervention is maintaining interest over time. QTC addresses this by its very nature – it invites the user into a long-term waiting game. After submitting a message, a user might forget about the site for some years, but the seed of awareness has been planted. If and when news about quantum computing breakthroughs appears (e.g. “researchers factor a 2048-bit RSA number on a quantum computer”), those who have used QTC may recall that they have a personal stake in the development. In this way, the project aims to sustain engagement passively: the users become part of a community of “time capsule contributors” who will collectively be excited on the day the capsule opens. We have implemented an email notification system as a gentle retention mechanism – users can opt in to be notified of major milestones or the final decryption event. This ensures that the educational impact can resurface years later at the teachable moment when quantum decryption becomes possible. In educational terms, QTC creates a *deferred lesson*: the real punchline (the revealing of messages) might occur decades in the future, at which point the significance of Shor’s algorithm will be viscerally demonstrated to all participants.

In summary, the pedagogical approach of Quantum Time Capsule is to intertwine factual learning with emotional storytelling. By giving the public a personal connection to an otherwise esoteric scientific development, we aim to demystify quantum computing and highlight its implications in a way that is both memorable and meaningful. Early usage data and feedback hint at the promise of this approach, and we anticipate that its impact will grow as the project matures and more people “lock” their secrets away for the quantum age.

Future Work

Quantum Time Capsule is an ongoing project, and we envision several enhancements that could enrich its educational value and user experience. In this section, we outline three major avenues for future work: (1) integrating a Shor’s algorithm emulator or visualization into the platform, (2) adding a post-quantum encryption option to contrast with the breakable RSA time capsules, and (3) developing user accounts and dashboards for long-term engagement.

**Shor’s Algorithm Emulator:** One limitation of the current QTC implementation is that the quantum decryption process remains a black box to users – we tell them *what* will eventually happen (a quantum computer will factor the RSA key) but not *how*. To address this, we plan to include an interactive **Shor’s algorithm emulator** as a learning module on the site. This module would allow users to input a much smaller RSA number (say 3 or 4 digits) and then step through the stages of Shor’s algorithm (modular exponentiation, quantum Fourier transform, period finding, etc.) in a visual manner. By doing so, users could grasp the essence of how quantum factoring works, seeing why quantum resources can succeed where classical brute force fails. Several research and educational tools for simulating Shor’s algorithm already exist; we could adapt an existing library or visualization for seamless integration. For instance, a user might select a small number like 15 or 21, and the tool would demonstrate finding its factors (3×5, 3×7) via quantum period-finding. This would reinforce the concepts introduced in the “How it works” text with an active learning exercise. While a full-scale simulation of RSA-4096 is impossible, even a toy demonstration would deepen appreciation for the quantum side of the time capsule story. It also provides an opportunity to explain concepts like qubits, superposition, and interference in the context of a concrete task (factoring), which can be more illuminating than treating those concepts in isolation.

**Post-Quantum Encryption Module:** Another planned feature is a **post-quantum crypto companion** to the time capsule. Currently, all messages in QTC are intentionally encrypted with an algorithm (RSA) that will become insecure in the future. As a counterpoint, we want to offer users the ability to also encrypt a message using a quantum-resistant algorithm – for example, using one of NIST’s selected post-quantum public-key schemes (such as CRYSTALS-Kyber for encryption). This would create a parallel “quantum safe” time capsule. Users could then choose: do they want their message to be readable in the future (use RSA and await Shor’s algorithm), or do they want it to remain secret indefinitely (use a post-quantum scheme that even quantum computers presumably cannot break)? This feature would serve as a pedagogical foil to the main QTC narrative. It would highlight the existence of solutions to the quantum threat, reinforcing that RSA’s vulnerability is not the end of secure communication​

[csrc.nist.gov](https://csrc.nist.gov/projects/post-quantum-cryptography)

. In practice, implementing a post-quantum encryption on the client side might involve using WebAssembly or JavaScript versions of lattice-based encryption algorithms. We would present it in a user-friendly way: perhaps a toggle or dropdown where the user selects “Quantum-vulnerable (RSA)” vs “Quantum-safe (PQC)” encryption for their message. The site could then generate two ciphertexts and explain that one is a **time capsule** and the other is a **tomb** (to use a metaphor: one will be opened by future quantum archeologists, the other is meant to remain buried forever). This comparison could spur discussions on the trade-offs and performance of post-quantum cryptography. It directly ties into ongoing real-world cryptographic transitions, thus broadening the educational scope of QTC from just illustrating the problem to also showcasing the solution.

**User Accounts and Dashboards:** As the number of participants grows, we see value in developing a more community-oriented aspect to QTC. Currently, a user interaction is stateless (once they encrypt a message and perhaps bookmark the ciphertext, their involvement ends until the decryption event). We plan to introduce optional **user accounts** or an identity mechanism where users can register (with minimal info) and manage their time capsule entries. A logged-in user could have a personal dashboard showing all the messages they have submitted, along with metadata such as submission date and perhaps an estimated “quantum unlock year” based on the latest quantum progress projections​

[quantumtimecapsule.com](https://quantumtimecapsule.com/explore_more)

. This dashboard could also display aggregate stats (e.g., “You are participant number X out of Y total; your message is one of Z messages this month”) to give users a sense of being part of a larger project. Additionally, we might allow users to write a short public blurb or title for their message (without revealing the secret itself) and opt-in to share it on a public “wall”. This would create a gallery of time capsule entries – e.g., someone might title their message “Letter to my 50-year-old self, written at 25” – which can inspire others and build anticipation. Community features like commenting or “liking” could even be considered, though moderation and privacy would need careful handling. The overarching goal of user accounts is to sustain engagement: instead of a one-off visit, users might return periodically to check their dashboard or see news updates about quantum computing on the QTC site. If major advancements occur (for example, a new record in quantum factoring), we could push notifications or highlight this news in user dashboards, contextualizing what it means for their time capsule. By nurturing a community of enthusiasts following the quantum timeline, QTC can evolve from a static website into a living platform for quantum awareness.

Beyond these main enhancements, there are other future directions worth exploring. We plan to collaborate with educators to incorporate QTC as a classroom activity in high school and university courses (for instance, as an introductory exercise in a lesson on cryptography: students create time capsules and then learn why they cannot open them without quantum computing). We also aim to localize the site into multiple languages to reach non-English-speaking audiences fascinated by technology and the future. On the technical front, if quantum simulators or small quantum computers become accessible via the cloud, we could attempt to factor tiny RSA instances live, as a demo, directly on quantum hardware – further blurring the line between present and future in the time capsule narrative. All of these ideas would enhance QTC’s mission: to use the impending advent of Shor’s algorithm as a lens through which anyone can learn about and engage with quantum computing.

Conclusion

We have presented **Quantum Time Capsule** as a novel approach to quantum computing outreach, one that transforms the abstract notion of “quantum risk to cryptography” into a personal and narrative-driven experience. In doing so, we demonstrate that public engagement with quantum technology need not be limited to games, quizzes, or graphical simulations of qubits; it can also be achieved through storytelling and creative framing of real-world cryptographic challenges. QTC’s core premise – inviting users to encrypt a secret that only a future quantum computer can decipher – serves as a powerful conversation starter about quantum computing’s disruptive potential. The project reframes the development of Shor’s algorithm and quantum factoring from a purely technical milestone into a shared societal moment that individuals can look forward to (with a mix of excitement and caution). This narrative angle complements traditional educational methods and helps to **humanize** the implications of quantum breakthroughs.

Our implementation of the QTC platform illustrates how such an idea can be realized in practice with straightforward web technologies, while still respecting the serious security underpinning the concept. By using strong RSA encryption and not retaining any decryption capability, we ensured that each user’s time capsule is genuine – its secrecy is as enduring as the hardness of factoring. The simplicity of the user experience (type a message and hit encrypt) belies the depth of the concepts involved, which range from number theory to quantum physics. Yet, through careful explanation and the emotional hook of a delayed reveal, participants gain an intuitive understanding of those concepts. Early engagement metrics, though limited, suggest that the time capsule narrative attracts a segment of the public that is curious and motivated to learn about quantum computing. As the platform grows and incorporates additional features like a Shor’s algorithm emulator and post-quantum encryption comparisons, we expect it to become an even richer educational resource.

In conclusion, Quantum Time Capsule represents a fusion of pedagogy and narrative rarely seen in quantum outreach: it is at once a **teaching tool**, an **artistic expression** (of trust in future scientists), and a **community-building exercise** around the coming quantum era. The project’s long-term nature is symbolic of the quantum computing field itself – a gradual journey with a transformative payoff. If and when a quantum computer finally factors a 4096-bit RSA number, it will not only mark a triumph of technology but also a poignant moment for all QTC participants who get to unlock their decade-old secrets. Our hope is that, along the way to that moment, the Quantum Time Capsule will have educated and inspired many people, leaving them more informed about cryptography, more excited about quantum science, and more prepared for the quantum future. As Michele Mosca has urged, society must be proactive in addressing the quantum threat​

[cigionline.org](https://www.cigionline.org/articles/quantum-threat-cyber-security/)

; QTC contributes to this goal by ensuring the conversation is not confined to experts, but is accessible to everyone with a story to encrypt and a stake in the future.

**References**

R. L. Rivest, A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,” *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[people.csail.mit.edu](https://people.csail.mit.edu/rivest/Rsapaper.pdf)

P. W. Shor, “Algorithms for Quantum Computation: Discrete Logarithms and Factoring,” in *Proc. 35th Annual Symposium on Foundations of Computer Science (FOCS)*, 1994, pp. 124–134.

[quantumalgorithmzoo.org](https://quantumalgorithmzoo.org/)

M. Mosca and B. Munson, “The Quantum Threat to Cyber Security,” *Centre for International Governance Innovation (CIGI)*, Oct. 2019.

[cigionline.org](https://www.cigionline.org/articles/quantum-threat-cyber-security/)

M. Mosca and M. Piani, *Quantum Threat Timeline Report 2022*. Global Risk Institute, Dec. 2022.

[quantumtimecapsule.com](https://quantumtimecapsule.com/explore_more)

NIST, “Post-Quantum Cryptography Standardization: Final Round Status,” National Institute of Standards and Technology, 2022.

[csrc.nist.gov](https://csrc.nist.gov/projects/post-quantum-cryptography)

J. Ossorio, J.-F. Laprade, U. Stege, and H. A. Müller, “QuantumCrypto: A Web Framework for Quantum Cryptography Education,” in *Proc. IEEE Int’l Conf. on Quantum Computing and Engineering (QCE)*, 2024, pp. 7–16.

file-fwnrgbjsfuweskthj5m9d5

S. Norrie, A. Estey, H. Müller, and U. Stege, “QNotation: A Visual Browser-Based Notation Translator for Learning Quantum Computing,” in *Proc. IEEE Int’l Conf. on Quantum Computing and Engineering (QCE)*, 2024, pp. 25–33.

file-asa6c9aczmgambvq3gbfbk

Z. C. Seskir *et al*., “Quantum games and interactive tools for quantum technologies outreach and education,” *Optical Engineering*, vol. 61, no. 8, p. 081809, 2022.

[research.tudelft.nl](https://research.tudelft.nl/files/139555635/081809_1.pdf)