We propose investigating the utility of a "cryptographic heartbeat" for the Internet. This "heartbeat" would be some trusted well-defended server which would output a sequence of unpredictable random strings at a prescribed interval. For example, it might output 1024-unpredictable random bits every second, 24 hours a day. This server would be run as an internet service, and clients of this service would acquire various chunks of information from the heartbeat provider.

We propose that a motivated undergraduate investigate the following ideas:

1. Timestamping: if user A wants to guarantee that he generated some particular email message no earlier than time X, he could include the latest heartbeat value along with the message.

2. Time-release encryption: if user A wants to give an encrypted message to user B but ensure that user B cannot read it until time X, A could purchase from the heartbeat provider the cryptographic hash of the heartbeat value at time X (the provider knows all future values) along with the identity of A. A then encrypts using a prefix of this hash as a key, and sends the ciphertext to B. A nice advantage here is that even if user A reneges or goes out of business, B will still uncover the message contents at the appointed time. Also, A and B are assured that no one else sees the secret message.

3. There are implications on the practicalities of non-interactive zero-knowledge proof protocols as well, where user A proves a fact to user B without revealing information he wishes to conceal.

Nominally, the benefits which might be realistically expected from these investigations include

1. Increasing our understanding of which protocols can be helped by such services,

2. Producing publications in this area to foment additional research,

3. Software tools which would either be directly deployable or at least simulate the objects involved in order to evaluate the practicality of these ideas,

4. Expose undergraduates to a unique area of computer science which combines mathematics with software and hardware concerns.