Q1: Protocols

Protocols are an established format of communication, in that protocols direct the exact methodology for the nature of the communication to take place. Specifically within a secured cryptographic context, a protocol will often define how an encryption algorithm will be executed for a transmission to take place.

Various cryptographic protocols are in use today, from key agreements in encrypting messages, to authentication methods for secured entry into a database for example, non repudiation methodologies, secure multiplex computations and communications for military-grade communications, as well as secured application-level topography for the data transport, as is often the case when using web-based platform services.

Properties of a protocol ensure the validity of the communication format. Everybody involved (Alice and Bob in our classroom examples) must (a) know the protocol and all of its steps, and (b) agree to follow these steps. In addition, (c) the protocol must be unambiguous and clearly defined, so that there is no chance of misunderstandings in the communication of information, or the transmission of data that envelopes the internal communication. Finally, (d) the protocol must be complete, in that for every possible scenario, there is one and only one outcome available. (Singh, 293-300)

Q2: ENIGMA

Authur Scherbuis's Enigma machine was a triumph of engineering and a valuable tool in the German war effort, having been defeated in large scale in the first world war and so with an obvious motivation for revenge and final vindication. The components that made up Enigma consisted of three parts: a keyboard for inputting plaintext, a scrambling unit that performed the encryption, and a display board that displayed the output letter for the ciphertext. An electrical signal would be sent as input through the keyboard, transmitting through the circuitry, and would be displayed via a series of lights at the top of the board.

Detailed technical aspects of the machine:

What kind of onion layers of security were built into the machine? As previously mentioned and per our text "The Code Book" cited in footnotes, the interface consisted of wiring connected to a the input: a typewriter-like keyboard for the input of plaintext characters, and the output: a display board containing lights for the display of the ciphered letter. Underneath that apparatus lied the enigmatic or ghostlike qualities that enabled the machine to last so long and successfully during the effort. First, were a series of rotors situated above the lights that were changed daily according to a known table. Second were a series of telecom switchboard cables that a dual-plug wire would be hooked into to perform a substitution from one letter set to another. Third, a set of disks known as a scramblers or rotors were connected to the keyboard by electrical wiring, and were to … The quantity of rotors were to increase the complexity of the alphabet's encryption input up to that point by a^n, where a = the count of letters in a given alphabet, be it latin-based (at the time), ASCII or Unicode (in modern emulators and simulators) and n = the

number of rotors. Finally, the reflector doubled the complexity of the algorithm up to *that* point, sending the signal back through the scramblers along a different path from which the signals came.

All of these efforts aided in eliminating the elementary steps of frequency analysis, repetition, and the vulnerabilities posed by having a small key, as the ENIGMA clearly did not have a small key.

Players involved in development:

Arthur Scherbius (1878-1929 per wikipedia) and E. Richard Ritter founded Scherbius & Ritter of Berlin-Wansee (Germany). Herr Scherbius wanted to replace the systems he deemed inadequate that were in use during WW1, with advancements invented by him and others in order to produce a truly remarkable device via the layers of cryptography as described above.

Players involved in breaking the code:

The years between WW1 and WW2 proved vital for **Poland**, as peacetime enabled a [relatively] calm environment to reflect on the careful reverse-engineering of this marvelous device. (However, during the war, this effort was dutifully hastened, and ultimately led to victory). **Hans-Thino Schmidt** (1888 - 1943) approached the French and ultimately sold secrets regarding ENIGMA for $30,000.00 to the **French intelligence authorities**. Poland continued their mathematical reverse-engineering efforts until the occupation of the country in WWII, handing over to **Great Britain** the responsibilities of decryption for ENIGMA from both “Room 40” and

from Blechley Park in Buckinghamshire. They eventually succeeded, and thus the demise of the German war machine from the Allies was at hand.

Impact it had on the field of cryptology:

Again we see how human error can lead to the demise of an amazingly complex (at the time) device through the laziness and repetitiveness of certain German officers. However, the ENIGMA machine played a huge role in the field of cryptology, by having built-in several technological advancements far exceeding any cryptological methodologies prior to the dawn of the computing era. (Singh 143-159)

Q3: Major achievements

I. Marconi

Guglielmo Marconi (1874 - 1937) discovered and capitalized on a certain property of electrical currents, namely that of wireless radio signalling and propagation. In order to capitalize, he filed several patents from 1897 to 1926, and sought commercial application for his inventions, (See https://en.wikipedia.org/wiki/Guglielmo_Marconi#Patents for a comprehensive listing). It was not long before military use became obvious, but with one obvious flaw: that of enemy eavesdroppers to the broadcasted signal. During WW1 there was no immediate solution, and there were as described in our text, a series of failures as far as broken ciphers and intercepted messages were concerned.

II. Zimmerman

Arthur Zimmermann (1864-1940) was associated with the Zimmermann Telegram, and was employed by the German Empire for close to one year. During this time, Zimmerman was involved in a plot to aid the Mexican government with the annexation of Texas, New Mexico and Arizona. Overconfidence in the technology employed during these negotiations as intercepted by the British, the deal fell through, and no plans came to fruition because it would not be much longer because he would no longer hold the office of State Secretary for Foreign Affairs.

III. ENIGMA

As described in more detail with a related question on this exam, the ENIGMA machine was a triumph of the "mechanicalization of secrecy", that is, the many layers that Herr Arthur Scherbius employed into his machine, including the input (keyboard) and output functions (lighted letters), all the wiring employed, the plug-board at front, the rotors in the back, and the codebook that was regularly distributed in order to reset the ciphers. Defeated because of a betrayal by Hans-Thilo Schmidt for $30K to the French authorities, and the continued efforts of reverse-engineering by the Poles and later the British.

IV. Navajo Code Talkers

In a heroic and ingenious effort, the United States military used the distinct and unique linguistic properties and advantages of the Navajo language in order to further encode wartime strategies during WW2. Philip Johnston recognized a need for a less mechanized and vulnerable approach towards the transmissions of secure data, and introduced the military to the Navajo Code Talkers, whom the enemy could not understand! Their heroic efforts continue to be recognized and honored to this day.

V. Egyptian hieroglyphics

In the fine human tradition of reviving lost and ancient languages, we are introduced to Egyptian hieroglyphics, which died out largely due to actions taken by the early Christian Church. The Rosetta Stone was discovered as a potential link between modern linguistics and the ancient hieroglyphics as well as the demotic Coptic dialect, using Greek as the base language at the foundation of scholarly interpretation. (Singh 101-142)

Q5: Key Distribution

Key freshness:

Freshness of a key, or the frequency of key generation, plays a large part in the cryptographic field by setting back any efforts of brute-force attack that are played out on a system. Having a smaller key will enable a quicker transmission, while having a larger or "heavier" key will result in a greater security, as it will be harder to break. However the disadvantage is that if the message is sensitive enough to warrant a new key for each transmission, the cost of resources will be high with a heavier key. In an ideal key-agreement setting and protocol, no single party should be able to control what the values or properties of the key will be.

It is recommended to change the key (a modern online password being of course only one type of key, but a most prominent example) as often as is feasible in order to minimize exposure via brute force.

Key derivation:

Derivation and generation of the keys is contingent on the agreement of all parties involved, and the size of the keys will usually be linearly proportional to the value of the protected data or classification of the transmission. Rather than to reinvent the wheel here via the generation of an entire keyset, one can derive from an original Key(A,B) a session Key(Ses) together with a number used only once. Thus, each session key Key(ses) will maintain a freshness and unique value with which to perform a transaction between parties.

Key Distribution Centers (KDCs)

A KDC is a central entity within an organization, (or an external relationship outside of the organization in order to transfer risk, obviously depending on the nature of the organization), whom all parties trust per prior agreement(s). From this, we have a two-step key distribution framework as follows: (1) KDC sends an individual Key Encryption Key (KEK) to all users, then (2) the KDC sends session keys K(ses) to all users which are encrypted with the KEK.

Going forward, it is clear what the pattern is. From an initial environment of trust, we set up channels from which initial keys are sent, then build upon that success with secondary keys, and tertiary keys for even more security for the sake of the transmission(s). We limit our discussion of encryption here, for it is clear that security is even further enhanced by the layers of encryption placed upon the packets of transmission or data itself!

Differences and similarities between asymmetric and symmetric key distribution:

Differences to asymmetric key distribution are obvious in that different keys between Alice and Bob are distributed, or in a more general sense beyond the two-party alice and bob model: [Key(a), Key(b), Key(c), … , Key(n)] where n = number of parties. Alice will encrypt using Key(a) and Bob will decrypt using Key(b). An advantage to using asymmetric keys is a higher degree of security. A disadvantage to the asymmetric model is that more resources are used, resulting in a slower generation of keys. In a symmetric model, Key(m) is used to both encrypt and decrypt message m. Keys are harder to manage, but the process is hastened, which can be valuable for smaller organizations with needs for a lesser degree of security for their data than

larger enterprises would need. Similarities include a consistent key distribution model, depending on the organization's security topology, and also a key duration length, which is independent of whether Sym or Asym keys are used. Asymmetric key technologies also have the distinct honor of being the technical model from which almost all modern encryption methodologies are derived.

Man in the Middle (Oscar) challenge and solution

As per the youtube video demonstrated in class via paint colors, Alice and Bob will both have a similar resulting color C while Oscar is left with a mystery color M. This is based on modular arithmetic where for both Alice and Bob, K(a,b) generates [(alpha)^a]^b) mod p (and [(alpha)^b]^a) mod p respectively) where p is a sufficiently large prime number.

At right… Janus, the Roman god of beginnings and endings, gates, times, transitions, doorways or portals, etc. Depicted as two-faced since he looks to the future and past at the same time. I believe this was used in class to illustrate Oscar.

Process of generation of certificates

A Certificate Authority (CA) is most commonly used to form a mutual trust between transactions of two or more nodes within a network graph. The generation of certificates results from this CA issuing its own signature *sig* such that $Key_{CA} \Rightarrow Sig[K_{CA}](Key_{PUB})$, or that the private key of the authority is used to generate a signature for the CA as well as to issue a public key for both parties A and B. Alice and Bob will therefore use the authority of the CA to establish a mutual trust.

Public Key Infrastructure (PKI)

The PKI refers to the entire ecosystem of public keys generated by a certificate authority, while distributed with the manufacture and shipment of browser and related software packages. The security of a Diffie-Hellman Key Exchange (DHKE) is maintained in that the PK need only be set up once, at the time of software initialization. (Singh, p.250)

References:

Singh, S. (2000). *The Code Book: The Science of Secrecy From Ancient Egypt to Quantum Cryptography*. Anchor Books.