Practical Cryptographic Systems

Symmetric Cryptography IV, Asymmetric Cryptography I

Instructor: Matthew Green

Housekeeping

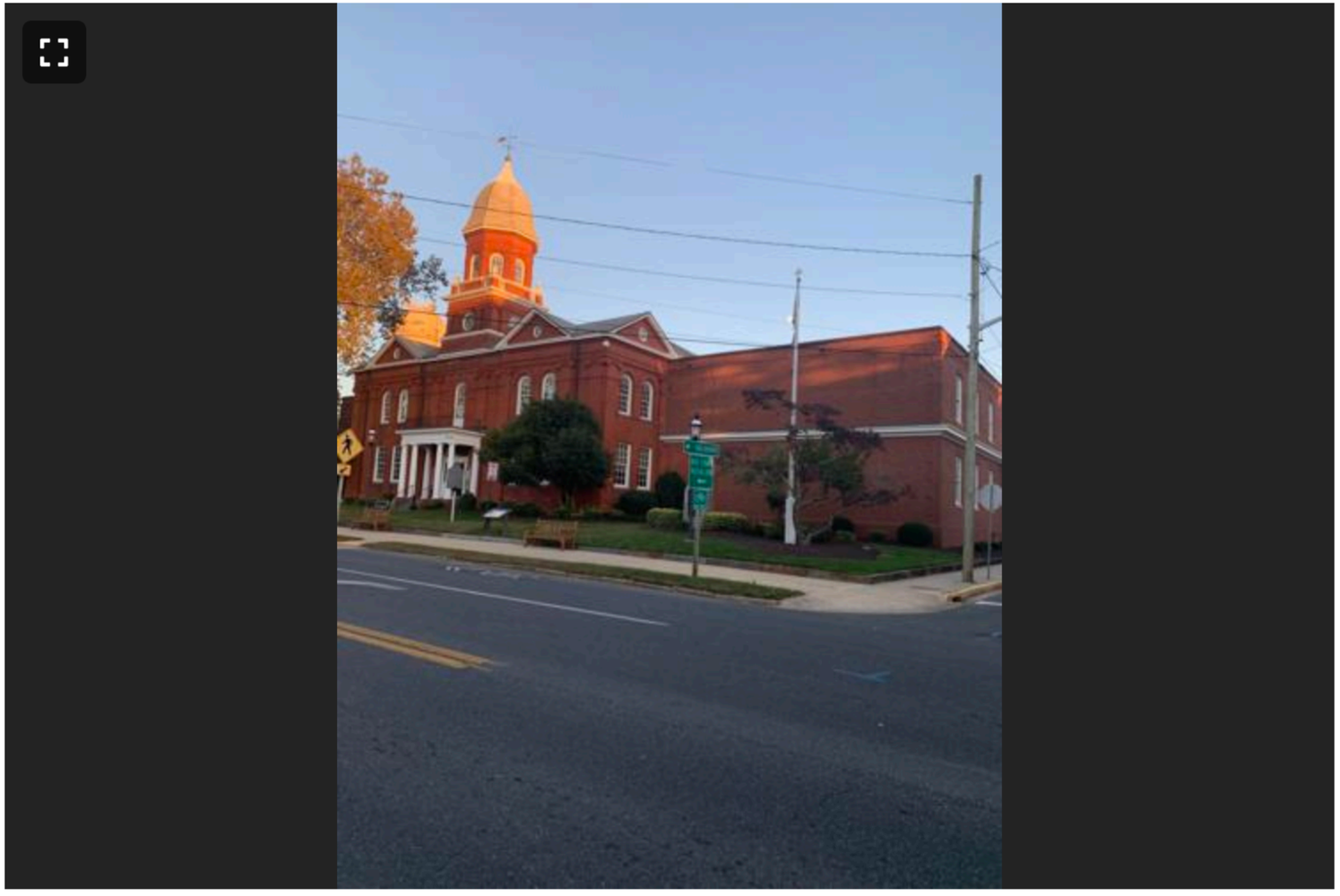
- Written assignment out today
  - **Take on Gradescope!**
  - **Note: there are separate Gradescope sections for 4xx, 6xx!**
  - Mostly based on Boneh-Shoup readings
- Project list updated
  - See course Github, main page
- Assignment 1 turn-in also available on Gradescope

News?

News?

Worcester Sheriff's Office still working on radio encryption

By Charlene Sharpe, Associate Editor Feb 1, 2024 Updated Feb 2, 2024 0



The Worcester County Sheriff's Office in Snow Hill

Weather

RIGHT NOW

42°

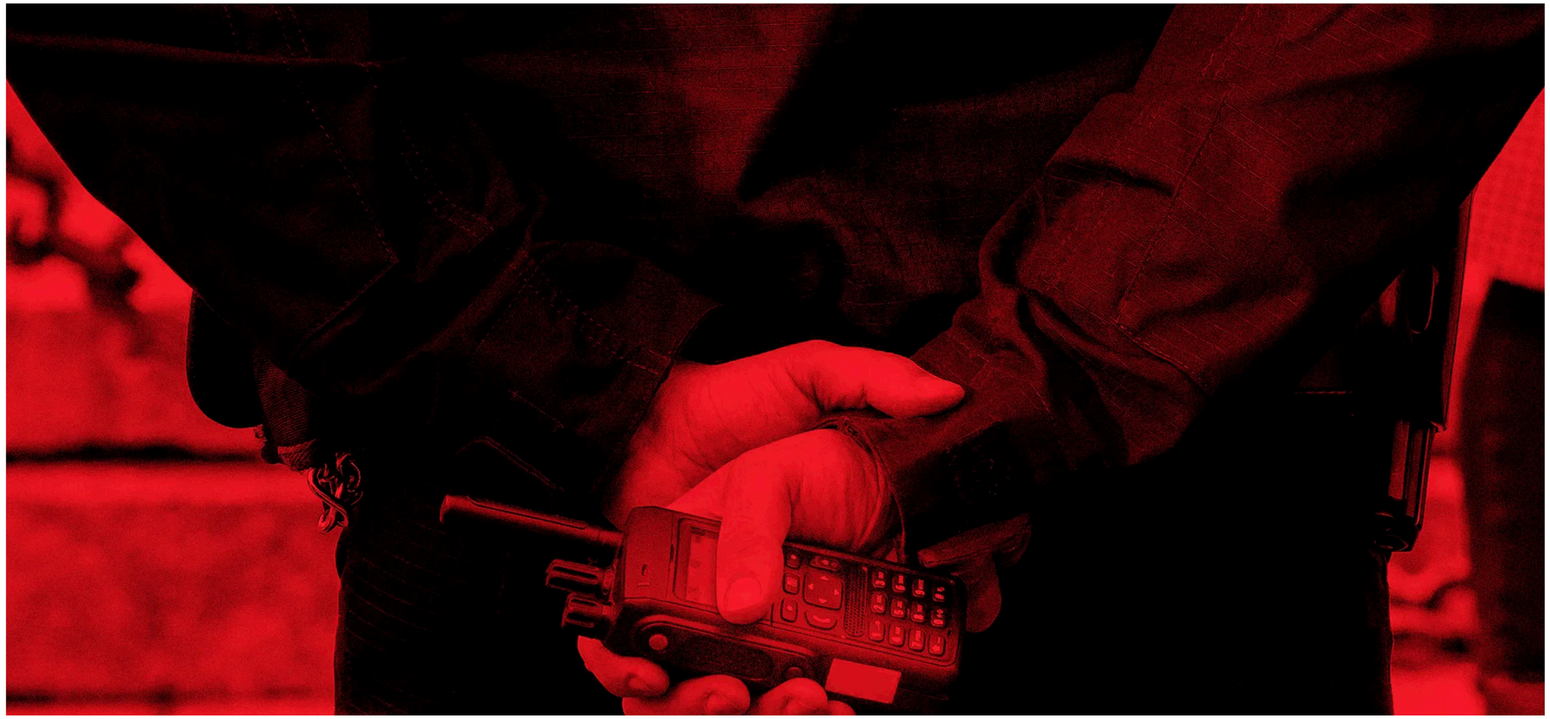
Sunny

Humidity: 60%
Cloud Coverage: 1%
Wind: 11 mph
UV Index: 3 Moderate
Sunrise: 07:02:05 AM
Sunset: 05:26:40 PM

KIM ZETTER SECURITY JUL 24, 2023 6:00 AM

Code Kept Secret for Years Reveals Its Flaw—a Backdoor

A secret encryption cipher baked into radio systems used by critical infrastructure workers, police, and others around the world is finally seeing sunlight. Researchers say it isn't pretty.



What we've covered so far

- Communication channels, adversaries
- Symmetric crypto:
  - Classical crypto, Vigenere, one-time pad ciphers
  - block ciphers (AES/DES), stream ciphers (AES-CTR, ChaCha20)
  - IND-CPA definition (semantic security)
  - Message Authentication Codes (MACs), to be cont'd

Ciphertext malleability

- The ability to modify a ciphertext
  - Such that the plaintext is meaningfully altered
  - CTR Mode (bad)
  - CBC Mode (somewhat bad)

Message Authentication Codes (MACs)

- Symmetric-key primitive
  - Given a key and a message, compute a “tag”

    MAC(k, M) -> T
  - Tag can be verified using the same key
    (usually we assume MAC is deterministic, and re-compute the tag)
  - Any changes to the message detectable
  - Why is this different than a CRC/checksum?

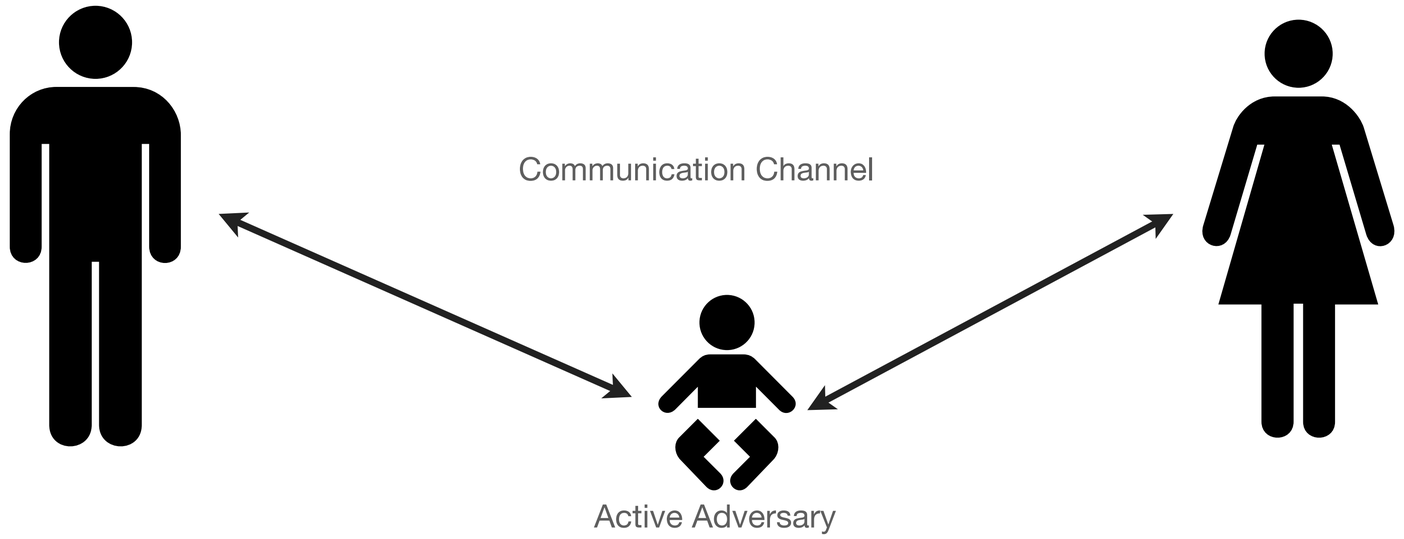
Message Authentication Codes (MACs)

- Examples of MACs:
  - HMAC (based on hash functions)
  - CMAC/CBC-MAC (based on block ciphers)
  - Polynomial MACs (based on polynomial arithmetic over rings, plus some pseudo randomness)
    e.g., the “G” in GCM mode, Poly1305

MACs

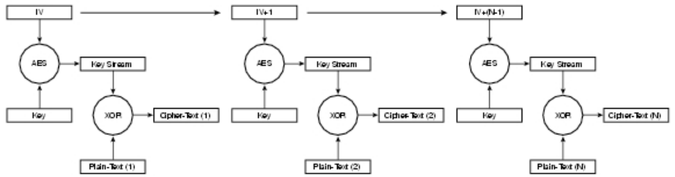
- Definitions of Security
  - Existential Unforgeability under Chosen Message Attack (EU-CMA)
  - (Note on replay attacks…)

Authenticated Encryption



Authenticated Encryption

- Two ways to get there:
  - Generic composition
    Encrypt (e.g., CTR mode) then MAC the cipher text
    (using two different keys!)
  - Authenticated mode of operation
    (e.g., GCM, CCM, OCB, ChaCha20-Poly1305)
    Integrates both encryption & authentication
    Single key, typically uses only one primitive



Hash Functions

Hash Functions

- Usually unkeyed*, converts variable-length string to small “tag”
  - Hash tables
  - Signatures
  - Software checksums
  - MAC functions (HMAC)
  - Encryption (OAEP)

Hash Functions

- Security properties:
  - Collision resistance
  - Pre-image resistance
  - Second pre-image resistance

Key distribution

- So far we've discussed symmetric crypto
  - Assumption is that both (all) parties share keys
  - Key distribution is a hard problem!
  - How do I get those keys?

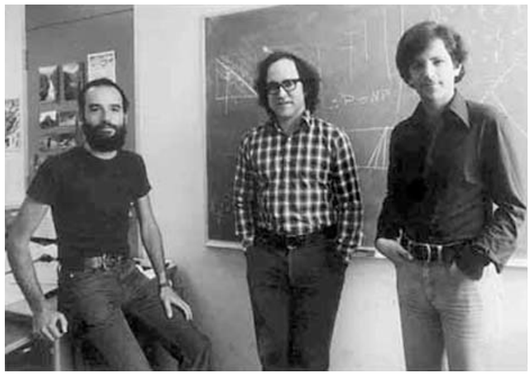
Key distribution: symmetric protocols

Key distribution: symmetric protocols

- Examples:
  - (Symmetric) Kerberos protocol
  - Needham-Schroeder

Asymmetric Crypto

- So far we've discussed symmetric crypto
  - Requires both parties to share a key
  - Key distribution is a hard problem!



Two slides of number theory

- Arithmetic modulo primes (Zp)

  1. What is Zp?
  2. Addition (+) and multiplication (*) in Zp
  3. Multiplicative inverses
  4. Z*p is the set of invertible elements (excludes 0)

See Boneh-Shoup, Appendix A

Two slides of number theory

- Cyclic groups

  1. A set of elements with a commutative “group operation”, identity element, at least one “generator” g
  2. Z*p is a cyclic group
  3. Not every element of Z*p is a generator
  4. Order: order(g) is number of elements generated, smallest element a s.t. g^a = 1
  5. Lagrange’s theorem: for all g \in Z*p, order(g) divides p-1
  6. Subgroups are subsets of a larger group that are also groups

See Boneh-Shoup, Appendix A