PAPER REVIEW OF: A METHOD FOR OBTAINING DIGITAL SIGNATURES AND PUBLIC-KEY CRYPTOSYSTEMS

Authors: R.L. Rivest, A. Shamir, and L. Adelman

By Amanda Lewis

FALL 2018 COSC 3325-02

PURPOSE AND MAIN ARGUMENT

- Written in 1977, when the world was transitioning from paper mail to an electronic mail system
- RSA authors wanted to preserve two important properties of the paper mail system:
  - Messages are private
  - Messages can be signed
- Public-key cryptosystem idea was invented by Diffie and Hellman, but never implemented before.

SUMMARIES

- Public-Key Cryptosystems
- Privacy
- Signatures
- Our Encryption and Decryption Methods
- The Underlying Mathematics
- Algorithms
- A Small Example
- Security of the Method: Cryptanalytic Approaches
- Avoiding "Reblocking" When Encrypting A Signed Message
- Conclusions

APPROACH

RESULTS

CONCLUSION

REFLECTION/COMMENTS