

גמג	שגמג	גג	גג	ששש	ההמגה	גג
לללל	לללללל	גל	מ	מגמג	מממ	מממ
לל	מ	מ	מ	ל	ל	ל
מ	מ	מ	מ	ל	ל	ל
מ	מ	מ	מ	מ	מ	מ
מ	מ	מ	מ	מ	מ	מ
מ	מ	מ	מ	מ	מ	מ
מ	מ	מ	מ	מ	מ	מ
מ	מ	מ	מ	מ	מ	מ
מ	מ	מ	מ	מ	מ	מ
מ	מ	מ	מ	מ	מ	מ

Susan Langford

# VERY simple substitution

- MS Word + esl\_gothic\_shavian.ttf
  - Arial: RONRIVEST
  - esl\_gothic\_shavian: RONRIVEST
- “Always check for plaintext”

# Plaintext

JSCJPYSDHEkSGYTkGROPRPVVDJRVSGRbSID  
bSHMHRObHROHHbPFMNPCRMkJSCDCCRTETkAMCPMSMT  
MSEbYCASIDYIMkJbNASMPMRFDVJ  
CFIPAMDkCDDPAbSFAOMbMFAOT  
RROWESMSkPPRJSAbkNEOCDSY  
PMEWJAASIVYDVSSWCPV  
VCPVVbWYIMPASRONRIVEST  
ADISHAMIRGIIIESbRASSARD

**JSCJPYSDHEkSGYTkGROPRPVVDJRVSGRbSID**  
**bSHMHRObHROHHbPFMNPCRMkJSCDCCRTETkAMCPMSMT**  
**MSEbYCASIDYIMkJbNASMPMRFDVJ**  
**CFIPAMDkCDDPAbSFAOMbMFAOT**  
**RROWESMSkPPRJSAbkNEOCDSY**  
**PMEWJAASIVYDVSSWCPV**  
**VCPVVbWYIMPASRONRIVEST**  
**ADISHAMIRGIIIESbRASSARD**

# Plaintext Source

## Session 1 *Random oracles*

09:10 - 09:35 ***The Random Oracle Model and the Ideal Cipher Model are Equivalent***

Best Paper Award

Jean-Sébastien Coron, Jacques Patarin, Yannick Seurin

09:35 - 10:00 ***Programmable Hash Functions and Their Applications***

Dennis Hofheinz and Eike Kiltz

10:00 - 10:30 **Morning Break**

## Session 2 *Applications*

10:30 - 10:55 ***One-Time Programs***

Shafi Goldwasser, Yael Tauman Kalai, and Guy Rothblum

10:55 - 11:20 ***Adaptive One-way Functions and Applications***

Omkant Pandey, Rafael Pass, and Vinod Vaikuntanathan