Scribe Notes for

RSA Encryption and Signatures

By Kevin Fournier

RSA
- Module $n$ where $n = pq$ and $p, q \rightarrow$ safe primes
- $pq \rightarrow (2p' + 1)(2q' + 1)$

Inverses
- Element $a \in \mathbb{Z}_n$ from $[0, \ldots, n-1]$
- $a$ is invertible iff $\gcd(a, n) = 1$
- Set of invertible elements is $\mathbb{Z}_n^*$

$\text{Ord}(a) | (p-1)(q-1) = \text{Ord}(a) | 4p'q'$

In general, $\text{Ord}(a) \mod(b) \rightarrow \text{Ord}(a) | \phi(b)$ where $\phi(b)$ is the number of integers less then $b$ and coprime to $b$.

Find $x$ given $g$ and $y$
- $y = xg \mod(n)$ Easy to find if $y$ is invertible, $y \in \mathbb{Z}_n^*$
- $y = gx \mod(n)$ Same as above
- $y = g^x \mod(n)$ Discrete log, still hard, $x = \log_g y$
- $y = x^g \mod(n)$ Discrete root, hard, $x = \sqrt[\varphi]{y}$

Given $n$ find $p$ and $q$
Factoring, hard
If the size of $n \geq 2048$, it takes $O(2^{112})$
$p$ and $q$ are usually the same length

Textbook RSA Encryption
Key Generation
1) Pick 2 large safe primes $p$ and $q$
2) Compute $n = pq$
3) Pick integer $e$ from $\mathbb{Z}_p^*$ which will be a public value
4) Compute $d = e^{-1} \mod((p-1)(q-1))$

Public Key: $(n, e)$
Private Key: $(d)$
Given $n$ it is infeasible to compute $(p-1)(q-1)$
$p$ and $q$ are secret but can be discarded

$\text{Enc}_{pk}(m) = m^e \mod(n) = c$
$\text{Dec}_{pk}(m) = c^d \mod(n) = m^{ed} \mod(n) = m$
Can’t find \( m \) from \( c,n \) because of discrete roots
Can’t find \( d \) given \( e,n \) because of factoring

Not randomized: Can encrypt the same message and get the same cyphertext
Multiplicatively Homomorphic: \( \text{Enc}(m_1) \times \text{Enc}(m_2) = \text{Enc}(m_1 \times m_2) \)

Signatures
Recall 2 methods
1) ZKP that you know secret key bound to a message
2) Sign by decrypting (doesn’t work for Elgamal because of randomization)
   \( S = \text{Sign}_{\text{SK}}(m) = \text{Dec}_{\text{SK}}(m) \)
   \( \text{output}<m,S> = m^d \mod(n) \)
   \( \text{Verify}_{\text{PK}}(m,S): S^e \mod(n) = m’ \)
   \( (2S)^e \mod(n) = m^{2e} \mod(n) \)
   \( 2^e m^d = m^{2e} \)
   \( 2^e m = 2^e m \)

Strengthening RSA
Use padding scheme where the scheme is randomized an uses hash functions
\( \text{Enc}(m || \text{pad}(r)) \) -> OAE: Optimal Asymmetric Encryption padding
   -> CCA secure
\( \text{Sign}(m || \text{pad}(r)) \) -> PSS: Probabilistic Signature Scheme
   -> AS secure as Schnorr and DSA

Encryption: Security: Signatures: Security:
Textbook RSA OTS Textbook RSA Not secure
Elgamal CPA (u) RSA-PSS Secure
Twin Elgamal CCA (u) DSA Secure
(u) RSA-OAEP CCA Schnorr Secure
   (PKCS variant)
(u): commonly used

Key Establishment:
Diffie-Hellman (Textbook) Not secure, MITM attack vulnerable
Diffie-Hellman (Signature) Secure, server contributed randomness, forward secrecy
Encryption (Key transport) Secure

Full Encrypted Protocol
You want to connect to google securely
1) Get google’s public key, pKg
2) \( K = \) Key Establishment (pKg) where \( K \) is a shared secret key
3) \( K_{\text{Enc}}, K_{\text{Mac}} = \text{PRG}(K) \)
4) \( \text{Enc}_{K_{\text{Enc}}}(m || \text{Mac}_{K_{\text{mac}}} || \text{pad}) \)