Problem with ElGamal Signature Scheme

- needs signature twice as large as its message.
- in order to be secure, one needs the prime modulus p of size 1024 bits. (Hence, 2048 bits signature)
  - maybe too large for certain applications
  - e.g. smart cards need shorter signature
- No hash function is built-in in the signature scheme.

Variants of ElGamal signature scheme

- Schnorr Signature Scheme
  - use of hash function
  - greatly reduce the signature size
- Digital Signature Algorithm (DSA)
  - published as adopted as a standard in 1994
  - incorporated the Schnorr Signature Scheme

Schnorr Signature Scheme (Motivation)

- $\mathbb{Z}_p^*$ is a cyclic group of order $p-1$.
- Let a prime $q | (p-1)$, q is large but it is much smaller than p.
- Let $\alpha \in \mathbb{Z}_p^*$ and its order is q. (how?)
  - That is, $<\alpha>$ is a subgroup of $\mathbb{Z}_p^*$ with q elements.
  - $\alpha = g^{p-1}/q$, g is a generator for $\mathbb{Z}_p^*$.
- $K = (p, q, \alpha, \beta; \beta = \alpha^a \mod p)$, only a is private.
- $h(x) \in \mathbb{Z}_q^*$ is a secure hash function.
- $k=$random selection from $\mathbb{Z}_q^*$,
Schnorr Signature Scheme  
(Motivation)

\[ \text{sig}_K(x, k) = (r, \delta) \]

- \[ r = h(x || (\alpha^k \mod p)) \]
- \[ \delta = k + a \cdot r \mod q \]

- choose \( \delta \) so that \( (\beta^\delta - r \cdot \alpha^\delta = \alpha^k) \mod p \).
- note that \( (\alpha^r \cdot \alpha^\delta = \alpha^\delta) \mod p \).
- how about \( \text{ver}_K(x, (r, \delta)) \)?

\[ \text{ver}_K(x, (r, \delta)) = \text{true}, \text{ if } h(x || (\beta^r \cdot \alpha^\delta \mod p)) = r. \]

Q: why not simply \( (\beta^r \cdot \alpha^\delta = \alpha^k) \mod p \)?

Schnorr Signature Scheme  
(Cryptosystem 7.3)

\[ K = \{ (p, q, \alpha, a, \beta) : \beta = \alpha^a \mod p \}, \]

- only \( \alpha \) is private. \( k \) = random from \( \mathbb{Z}_q^* \).

\[ \text{sig}_K(x, k) = (r, \delta) \]

- \[ r = h(x || (\alpha^k \mod p)) \]
- \[ \delta = k + a \cdot r \mod q \]

[So that \( (\beta^\delta - r \cdot \alpha^\delta = \alpha^k) \mod p \).]

\[ \text{ver}_K(x, (r, \delta)) = \text{true}, \text{ if } h(x || (\beta^r \cdot \alpha^\delta \mod p)) = r. \]

Schnorr Signature Scheme  
Parameters

\[ p \approx 2^{1024}, q \approx 2^{160}. \text{ (so that SHA-1 can be used as a secure hash function)} \]

- \( q \mid (p-1) \). it is easier to fix \( q \) and then search for a prime \( p \) of the form \( p = cq + 1 \).

We can find \( \alpha \) of order \( q \) by

- \( \alpha = g^{(p-1)/q}, g \) is a generator for \( \mathbb{Z}_p^* \).

(why?)
Example 7.3

K=((p, q, a, b); \beta= \text{or mod } p), \alpha=\text{or mod } q, \beta= a \text{ mod } p, \alpha=\text{or mod } q, \beta= a \text{ mod } p.

\text{Example 7.4}

K=((p, q, a, b); \beta= \text{or mod } p), \alpha=\text{or mod } q, \beta= a \text{ mod } p, \alpha=\text{or mod } q, \beta= a \text{ mod } p.
Elliptic Curve DSA (ECDSA)
- ECDSA was approved as in FIPS 186-2 in 2000.
- DSA: $a^k \mod p$ vs. ECDSA: $kA$
  - multiplicative group vs. additive group.
- See Cryptosystem 7.5. (page 298)
- (skip)

Elliptic Curves (Review)
- $y^2 = x^3 + a x + b,$ where
  - $4a^3 + 27b^2 \neq 0.$
- EC Curve over real (Fig 6.1, page 256)
- Result of $P_1 + P_2$ is shown.

Elliptic Curves Over $\mathbb{Z}_p$
- $y^2 = x^3 + a x + b,$ where
  - $4a^3 + 27b^2 \neq 0.$
- EC Curve over $\mathbb{Z}_p$ or a finite field can be similarly defined. We can show that it is a group in which DL problem is also intractable. (skip)
**Provably secure signature schemes**

- One-Time Signature
  - Cryptosystem 7.6 (page 300)
- Full Domain Hash
  - Cryptosystem 7.7 (page 304)
- (skip)

---

**Undeniable signatures**

- Chaum and Antwerpen (1989).
- Requires cooperation of the signer (A) to verify the signature.
  - using challenge-and-respond protocol.
  - most ElGamal-like signature scheme has pair of as signature for x: (x, (r, δ))
  - easy to copy (x, (r, δ)) w/o A approval.
  - only one part of the signature given.

---

**Chaum and Antwerpen Signature Scheme Parameters**

- Similar to Schnorr scheme except that p=2q+1.
- Let \( a \in \mathbb{Z}_p^* \) and its order is q. (how?)
  - \( a = g^{(p-1)/q} = g^2 \), g is a generator for \( \mathbb{Z}_p^* \).
- \( K = \{(p, q, a, \alpha, \beta) : \beta = \alpha^a \mod p\} \), only \( a \) is private.
- Signature: \( y = \text{sig}_a(x) = x^a \mod p \).
  - (similar but not quite as RSA signature)
Chaum and Antwerpen
Signature Scheme Features

- B (Bob) received \( y = \text{sig}_K(x) = x^a \mod p \), supposedly signed/sent from A (Alice).
- \( y \) can be a forgery or a valid signature
- B issues a challenge to A for a response to either verify \( y \) is valid signature or \( y \) is indeed a forgery.
- Q: what if A wants to disavow her own signature?

Cryptosystem 7.8: Chaum and Antwerpen Signature Scheme

\[ K = \{(p, q, a, \beta) : \beta = a^\alpha \mod p \}, \text{ only } a \text{ is private. } q = (p-1)/2, \ a = g^2 \mod p. \]

Signature: \( y = \text{sig}_K(x) = x^a \mod p \).

Verification:
1. B chooses \( e_1, e_2 \) randomly from \( Z_q^* \).
2. B computes \( c = y^{e_1} \beta^{e_2} \mod p \), send to A.
3. A computes \( d = c^A \mod p, A = a^{-1} \mod q \).
4. B accepts \( y \), whenever \( d = x^{e_1} \beta^{e_2} \mod p \).

Example 7.7 (page 309)

\[ K = \{(p, q, a, \beta) : \beta = a^\alpha \mod p \}, \text{ a is private. } q = (p-1)/2, \ a = g^2 \mod p. \]

Signature: \( y = \text{sig}_K(x) = x^a \mod p \).

Verification:
1. B chooses \( e_1, e_2 \) from \( Z_q \).
2. B computes \( c = y^{e_1} \beta^{e_2} \mod p, \) send to A.
3. A computes \( d = c^A \mod p, A = a^{-1} \mod q. \)
4. B accepts \( y \), whenever \( d = x^{e_1} \beta^{e_2} \mod p. \)
Disavow Protocol

- What if \(d \neq x^a \cdot y^e \mod p\) in the Cryptosystem 7.8?
  1. \(y\) may be forgery and indeed not signed by \(A\). \(A\) can convince \(B\) that it is indeed a forgery. (how? why?)
  2. \(y\) may be signed by \(A\) but for some reason, \(A\) would like to disavow. The chance of “successful denial” is small.

Algorithm 7.3 Disavowal

Consist of two runs of verification and one run consistency check.

1. \(B\) chooses \(e_1, e_2\) from \(Z_q^*\).
2. \(B\) computes \(c = y^{e_1} \cdot y^{e_2} \mod p\), send to \(A\).
3. \(A\) sends \(B\) with \(d = c^a \mod p\), \((A = a^{-1} \mod q)\).
4. \(B\) verifies \(d \neq x^{e_1} \cdot y^{e_2} \mod p\).

1. \(B\) chooses \(f_1, f_2\) from \(Z_q^*\).
2. \(B\) computes \(C = y^{f_1} \cdot y^{f_2} \mod p\), send to \(A\).
3. \(A\) sends \(B\) with \(D = C^a \mod p\), \((A = a^{-1} \mod q)\).
4. \(B\) verifies \(D \neq x^{f_1} \cdot y^{f_2} \mod p\).

\(B\) concludes \(y\) is a forgery if and only if \((d \cdot a^{-e_2}) \cdot f_1 = (D \cdot a^{-f_2}) \cdot e_1 \mod p)\)

Example 7.8 (page 311)

1. \(B\) chooses \(e_1, e_2\) from \(Z_q^*\).
2. \(B\) computes \(c = y^{e_1} \cdot y^{e_2} \mod p\), send to \(A\).
3. \(A\) sends \(B\) with \(d = c^a \mod p\), \((A = a^{-1} \mod q)\).
4. \(B\) verifies \(d \neq x^{e_1} \cdot y^{e_2} \mod p\).
5. \(B\) chooses \(f_1, f_2\) from \(Z_q^*\).
6. \(B\) computes \(C = y^{f_1} \cdot y^{f_2} \mod p\), send to \(A\).
7. \(A\) sends \(B\) with \(D = C^a \mod p\), \((A = a^{-1} \mod q)\).
8. \(B\) verifies \(D \neq x^{f_1} \cdot y^{f_2} \mod p\).

Show that, \(f_1 = 125, f_2 = 9\), \(C = 270\), \(D = 68\).

\(B\) concludes \(y\) is a forgery if and only if \((d \cdot a^{-e_2}) \cdot f_1 = (D \cdot a^{-f_2}) \cdot e_1 \mod p)\)

\((109 \cdot 4^{125}) \cdot 125 = (68 \cdot 4^9) \cdot 9 = 188 \mod 467,\)
**Theory behind Chaum and Antwerpen Signature Scheme**

Theorem 7.3 (page 309):
- If \( y \neq x^a \mod p \), then B will accept \( y \) as a valid signature for \( x \) with prob. \( \leq 1/q \).

Theorem 7.4 (page 311):
- If \( y \neq x^a \mod p \), both A and B follow Disavow Protocol, then
  \[
  (d^{-e_2}) f_1 = (D^{-f_2}) e_1 \pmod{p}
  \]

Theorem 7.5 (page 312):
- If \( y = x^a \mod p \), (true sig. of A) and B follows Disavow Protocol (A may not follow and send B: \( d \) and \( D \)), and
  1. B verifies \( d^{e_1} a^{e_2} \mod p \).
  2. B verifies \( D^{f_1} a^{f_2} \mod p \).
- Then \( \Pr(\text{not EQ}) = 1-1/q \), \( \Pr(\text{EQ}) = 1/q \).
  \[
  \text{EQ: } (d^{-e_2}) f_1 = (D^{-f_2}) e_1 \pmod{p}
  \]

**Fail-stop signatures**
- provides enhanced security against the possibility that a very powerful adversary might be able to forge a signature.
- (skip)
Summary

- Variants of ElGamal signature scheme
  - Schnorr signature scheme
  - DSA: Digital Signature Algorithm
- Provably secure signature scheme (skip)
- Undeniable signature
  - features and applications
- Fail-stop signature (skip)

HW 7

- Chapter 7: 7.1, 7.4, 7.7, 7.15.