Algorithms of Information Security: Cryptographic Protocols

Faculty of Information Technology
Czech Technical University in Prague

November 10, 2022

Interactive proof system.

- Interactive proof system.
- Zero knoweledge proof protocol.

Squares and square roots.

- We have a function $x \mapsto x^2 \mod n$ and its inverse is a function $y \mapsto \sqrt{x} \mod n$.
- An integer b is a square root of a modulo n, if

$$b^2 = a(\text{ mod } n).$$

- Let $a \in \mathbb{Z}$ and $n \in N$. We say that a is a quadratic residue modulo n if there exists $b \in N$ such that $b^2 = a(\text{ mod } n)$. Otherwise, we say that a is a quadratic nonresidue.

Quadratic residues.

- We partition Z_n^* into two parts.
  - $QR_n = \{a \in Z_n^* \mid a \text{ is a quadratic residue modulo } n\}$.
  - $QNR_n = Z_n^* - QR_n$.
- QR_n is the set of quadratic residues modulo n.
- QNR_n is the set of quadratic non-residues modulo n.

Facts. Let $n = pq$, where p and q are different odd primes.

- Every $a \in QR_n$ has exactly four square roots in Z_n^*.
- Exactly $(p-1)\cdot(q-1)/4$ of the elements of Z_n^* are quadratic residues.

For an odd prime p holds:

- Every $a \in QR_p$ has exactly two square roots in Z_p^*.
- Exactly $1/2$ of the elements of Z_p^* are quadratic residues.

Protocol Feige-Fiat-Shamir.

- The Feige-Fiat-Shamir protocol is based on the difficulty of computing square roots modulo composite numbers.
- Alice chooses $n = pq$, where p and q are distinct large primes.
- Next she picks a quadratic residue $v \in QR_n$.
- Finally, Alice chooses s to be the smallest square root of $v^{-1} (\bmod n)$.
  Note. Note that if v is a quadratic residue, then so is $v^{-1} (\bmod n)$.
- Next, she publishes n and v and keeps s as her private secret.

A simplified one-round FFS protocol.

- Alice chooses random $r \in Z_n^*$. Next, compute $x = r^2 (\mod n)$ and send x to Bob.
- Bob chooses a random $b \in \{0, 1\}$ and sends b to Alice.
- Alice computes $y = rs^b (\mod n)$ and sends y to Bob.
- If $b = 0$, Bob checks if $x = y^2 (\mod n)$. If $b = 1$, Bob checks if $x = y^2 v (\mod n)$.

Protocol Feige-Fiat-Shamir (FFS).

We make three claims for the FFS protocol.

- (Completeness) When both Alice and Bob are honest, Bob's check always succeeds.
- (Soundness) If Eve attempts to impersonate Alice without knowing her secret, Bob's check will fail with probability at least 1/2.
- (Zero knowledge) Anything that Eve can compute while interacting with Alice in the FFS protocol can also be computed without Alice's involvement. Specifically, if Eve can find Alice's secret s after running the FFS protocol, then she could have found s without ever talking to Alice.

Protocol FFS. Completeness.

- When both parties are honest, Bob checks

$$x = y^2 v^b (\bmod n)$$

and succeeds because

$$y^2 v^b = (rs^b)^2 v^b = r^2 (s^2 v)^b = x (v^{-1} v)^b = x (\bmod n).$$

- We will look at the two cases separately:
  - $b = 0:$ Then $y = r$ a $y^2 = r^2 = x(\bmod n)$.
  - $b = 1:$ Then $y = rs(\bmod n)$ and $s^2 = v^{-1}(\bmod n)$, so

$$y^2 v = r^2 s^2 v = r^2 (v^{-1} v) = r^2 = x (\bmod n).$$

Protocol FFS. Soundness.

- *Theorem.* Suppose Eve does not know the square root of v^{-1}. Then Bob's verification fails with probability at least 1/2.
- *Proof.* To successfully fool Bob, Eva must come up with x in step 1 and y in step 3 satisfying $x = y^2 v^b (\mod n)$.
- In the 1st step, Eve sends x even before Bob chooses b. So she does not know what value of b to expect.
- When Eve receives b, she responds by sending the value of y_b to Bob.

Protocol FFS. Soundness.

We consider two cases.

- Case 1. There exists at least one $b \in \{0, 1\}$ for which y_b does not satisfy $x = y^2 v^b (\mod n)$. We know that each of the possibilities $b = 0$ or $b = 1$ occurs with probability 1/2, that is, Bob's verification fails with probability at least 1/2 as desired.
- Case 2. y_0 and y_1 both satisfy the verification equation, so $x = {y_0}^2 (\mod n)$ and $x = {y_1}^2 v (\mod n)$. Then we can solve these equations for v^{-1} and get

$$v^{-1} = {y_1}^2 x^{-1} = {y_1}^2 {y_0}^{-2} (\mod n).$$

Then $y_1 {y_0}^{-1} (\mod n)$ is the square root of v^{-1}.
Since Eve would be able to calculate both y_0, and y_1, then she would also be able to calculate the square root of v^{-1} , which contradicts the assumption that she doesn't "know" the square root of v^{-1}.

Protocol FFS. Successful cheating with probability 1/2.

We note that it is possible for Eva to cheat with a probability of success of 1/2.

- She guesses the bit b, that Bob sends her in step 2 and generates the pair (x, y).
- If she guesses $b = 0$, then she chooses $x = r^2(\mod n)$ and $y = r(\mod n)$, just like Alice would have done.
- If she guesses $b = 1$, then she chooses y arbitrarily and $x = y^2 v(\mod n)$.

She proceeds to send x in step 1 and y in step 3.
Bob accepts the pair (x, y), if Eve guesses b correctly, which happens with probability 1/2.

Protocol FFS. Zero knowledge.

- We now consider the case where an honest Alice interacts with a dishonest Eve who pretending to be Bob, or simply a dishonest Bob who wants to capture Alice's secret.
- Alice would like to be sure that her secret is protected if she follows the protocol, no matter what Eve (or Bob) does.
- What does Eva know at the end of the protocol?

Protocol FFS. Zero knowledge.

- Suppose, that Eva sends $b = 0$ in step 2.
- Then she ends up with a pair (x, y), where y is a random number and x is its square modulo n.
- Neither of these numbers depend in any way on Alice secret s, so Eva gets no direct information about s.
- It is also useless for Eve to try to find s by other means, since she can calculate such pairs herself without involving Alice.
- If such pairs allowed her to find the square root of v^{-1}, then she would already be able to calculate square roots, which contradicts the assumption that finding square roots modulo n is difficult.

Protocol FFS. Zero knowledge.

- Suppose, that Eva sends $b = 1$ in step 2.
- Now she ends up with the pair (x, y), where $y = rs(\bmod n)$ and $x = r^2(\bmod n)$.
- While y might seem to give information about s, observe that y sitself is just a random element of Z_n^*. This is because r is random and the mapping $r \to rs(\bmod n)$ is one-to-one for all $s \in Z_n^*$. Hence, as r ranges through all possible values, so does $y = rs(\bmod n)$.
- Eva learns nothing from x that she could not have computed herself knowing y, for $x = y^2 v \bmod n$.
- Again, all she ends up with is a random number (in this case y) and the quadratic residue x, which she can compute knowing y.

Protocol FFS. Zero knowledge.

- In both cases, Eva ends up with information she could have calculated without interacting with Alice.
- So if Eve could have discovered Alice's secret by talking to Alice, she could have done it herself, which contradicts the assumption for calculating square roots.
- Alice's protocol releases zero knowledge about her secret.

Feige-Fiat-Shamir identification protocol.

- The basic version of the Fiat-Shamir protocol can be generalized, and the Feige-Fiat-Shamir identification Protocol (FSS) is a small modification of such a generalization.
- The FFS protocol involves identifying an entity by proving knowledge of a secret using a zero-knowledge proof. The protocol does not reveal any partial information regarding the secret identification values of A.
- It requires limited computation (a small fraction of that required by RSA), and is thus suitable for applications with low-power processors (eg, 8-bit smart card microprocessors).

Feige-Fiat-Shamir identification protocol

Algorithm 1 Feige-Fiat-Shamir identification protocol

SUMMARY. A proves knowledge of s to user B in t iterations of the 3-pass protocol.

1. *Selection of system parameters.* The trusted center T, after choosing two secret primes p and q each congruent to 3 modulo 4, publishes a common modulus $n = pq$ to all users, such that n is computationally infeasible to factorize. The integers k and t are defined as security parameters.

Feige-Fiat-Shamir identification protocol

Algorithm 2 Feige-Fiat-Shamir identification protocol

2. *Selection of per-user parameters.* Each entity A does the following.
   - It selects k random integers $s_1, s_2, \ldots, s_k$ in the range $1 \leq s_i \leq n-1$, and k random bits $b_1, \ldots, b_k$. (For technical reasons, required $gcd(s_i, n) = 1$, but this is almost certainly guaranteed since otherwise the number n can be factorized.)
   - Compute $v_i = (-1)^b_i \cdot (s_i^2)^{-1} \bmod n$ for $1 \leq i \leq k$.
   - A identifies itself by non-cryptographic means (e.g. ID card) T, with which it subsequently registers the public key $A : (v_1, \ldots, v_k; n)$, while only A knows its private key $(s_1, \ldots, s_k)$ and n. This completes the one-time setup phase.

Feige-Fiat-Shamir identification protocol

Algorithm 1 Feige-Fiat-Shamir identification protocol

3. *Protocol messages.* Each of t rounds has three messages as follows.

$$A \rightarrow B : x(= \pm r^2 \bmod n) \tag{1}$$

$$A \leftarrow B : (e_1, \ldots, e_k), e \in \{0,1\} \tag{2}$$

$$A \rightarrow B : y(= r \cdot \prod_{e_j=1} s_j \bmod n) \tag{3}$$

Feige-Fiat-Shamir identification protocol

Algorithm 1 Feige-Fiat-Shamir identification protocol

4. *Protocol actions.* The following steps are performed t times; B accepts the identity of A if all t iterations succeed. Assume that B has the authentic public key of $A : (v_1, \ldots, v_k; n)$; otherwise, the certificate can be sent in message (1).
   - A selects a random integer $r, 1 \leq r \leq n-1$, and a random bit b; calculates $x = (-1)^b \cdot r^2$ mod n and sends x (witness) to B.
   - B sends A (the challenge), a random $k-$bit vector $(e_1, \ldots, e_k)$.
   - A calculates and sends B (answer) $y = r \cdot \prod_{j=1}^{k} s_j^{e_j}$ mod n (the product of r with s_j determined by the challenge).
   - B calculates $z = y^2 \cdot \prod_{j=1}^{k} v_j^{e_j}$ mod n, and verifies that $z = \pm x$ and $z \neq 0$ (this rules out the adversary's success by choosing $r = 0$).

Example. Apply the Feige-Fiat-Shamir identification protocol if we know that the trusted center T has chosen the following secret primes: $p = 683$ and $q = 811$. We know that $k = 3$ and $t = 1$ and suppose A chose 3 the following random integers: $s_1 = 157, s_2 = 43215$ and $s_3 = 4646$ and 3 random bits $b_1 = 1, b_2 = 0$ and $b_3 = 1$. Next, suppose that $r = 1279, b = 1$ and we know that B will send A the following random vector $(0, 0, 1)$.

Feige-Fiat-Shamir identification protocol

Solution. We know that the trusted center T has chosen the following primes: $p = 683$ and $q = 811$. First, we check whether the primes p and q are each congruent 3 modulo 4. Both primes satisfy the given condition. The trusted center T had to publish $n = pq = 553913$, while the prime numbers p and q were not published by the trusted center T. Further, we know that $k = 3$ and $t = 1$ and suppose that A has selected 3 following random integers: $s_1 = 157, s_2 = 43215$ and $s_3 = 4646$ and 3 random bits $b_1 = 1, b_2 = 0$ and $b_3 = 1$. We need to check if $gcd(s_i, n) = 1$, for $1 \leq i \leq 3$. The given condition is satisfied by s_1, s_2 and s_3.

Feige-Fiat-Shamir identification protocol

Compute $v_i = (-1)^b_i \cdot (s_i^2)^{-1}$ mod n for $1 \leq i \leq 3$.

$$v_1 = (-1)^1 \cdot (157^2)^{-1} = 441845 \text{ mod } 553913$$
$$v_2 = (-1)^0 \cdot (43215^2)^{-1} = 338402 \text{ mod } 553913$$
$$v_3 = (-1)^1 \cdot (4646^2)^{-1} = 124423 \text{ mod } 553913$$

- The public key of A is $(v_1, v_2, v_3; n)$, i.e. $(441845, 338402, 124423; 553913)$.
- The private key of A is (s_1, s_2, s_3) i.e. $(157, 43215, 4646)$.

We have only $t = 1$ iteration which has three messages in the following form.

$$A \rightarrow B : x(= \pm r^2 \text{ mod } n) \quad (1)$$
$$A \leftarrow B : (e_1, \ldots, e_3), e \in \{0, 1\} \quad (2)$$
$$A \rightarrow B : y(= r \cdot \prod_{e_j=1} s_j \text{ mod } n) \quad (3)$$

Feige-Fiat-Shamir identification protocol

- We know that A chose $r = 1279$ and the random bit $b = 1$ further calculates $x = (-1)^b \cdot r^2 \bmod n$. So $x = (-1)^1 \cdot 1279^2 \bmod 553913$ and we send $x = 25898$ to user B.
- Suppose B sends A the following random $3-$bit vector $(0, 0, 1)$.
- A calculates and sends $B : y = r \cdot \prod_{j=1}^{k} s_j^{e_j} \bmod n$ i.e. $y = r \cdot s_3 \bmod n = 403104$.
- B calculates $z = y^2 \cdot v_3 \bmod n = 25898$ and accepts the identity A, since $z = +x$ and $z \neq 0$.

Guillou-Quisquater (GQ) identification protocol

- The Guillou-Quisquater (GQ) identification scheme is an extension of the Fiat-Shamir protocol.
- It allows a reduction in both the number of messages exchanged and memory requirements for user secrets and, like Fiat-Shamir, is suitable for applications in which the claimant has limited power and memory.
- It involves three messages between a claimant A whose identity is to be corroborated, and a verifier B.

Algorithm 2 Guillou-Quisquater (GQ) identification protocol

SUMMARY. A proves its identity (via knowledge of s_A) to B in a 3-pass protocol.

1. *Selection of system parameters.*
   - An authority T, trusted by all parties with respect to binding identities to public keys, selects secret random RSA-like primes p and q yielding a modulus $n = pq$. (As for RSA, it must be computationally infeasible to factor n.)
   - T defines a public exponent $v \geq 3$ with $\gcd(v, \phi) = 1$ where $\phi = (p-1)(q-1)$, and computes its private exponent $s = v^{-1}$ mod ϕ.
   - System parameters (v, n) are made available (with guaranteed authenticity) for all users.

Guillou-Quisquater (GQ) identification protocol

Algorithm 3 Guillou-Quisquater (GQ) identification protocol

2. *Selection of per-user parameters.*
   - Each entity A is given a unique identity I_A, from which (the redundant identity) $J_A = f(I_A)$, satisfying $1 < J_A < n$, is derived using a known redundancy function f.
   - T gives to A the secret (accreditation data) $s_A = (J_A)^{-s} \bmod n$.
3. *Protocol messages.* Each of t rounds has three messages as follows (often $t = 1$).
   - $A \to B : I_A,\ x = r^v \bmod n$
   - $A \leftarrow B : e$ (where $1 \leq e \leq v$)
   - $A \to B : y = r \cdot {s_A}^e \bmod n$

Guillou-Quisquater (GQ) identification protocol

Algorithm 3 Guillou-Quisquater (GQ) identification protocol

4. *Protocol actions.* A proves its identity to B by t executions of the following; B accepts the identity only if all t executions are successful.
   - A selects a random secret integer r (the commitment), $1 \leq r \leq n-1$, and computes (the witness) $x = r^v \bmod n$.
   - A sends to B the pair of integers (I_A, x).
   - B selects and sends to A a random integer e (the challenge), $1 \leq e \leq v$.
   - A computes and sends to B (the response) $y = r \cdot {s_A}^e \bmod n$.
   - B receives y, constructs J_A from I_A using f (see above), computes $z = {J_A}^e \cdot y^v \bmod n$, and accepts A's proof of identity if both $z = x$ and $z \neq 0$. (The latter precludes an adversary succeeding by choosing $r = 0$.)

Guillou-Quisquater (GQ) identification protocol

Example. Consider a Guillou-Quisquater (GQ) identification protocol between Alice and Bob with primes $p = 569, q = 739$ and $v = 54955, t = 1$ and Alice's redundant identity is $J_A = 34579$. Describe the communication between Alice and Bob if she chooses $r = 65446$ and the challenges $e = 38980$.

Guillou-Quisquater (GQ) identification protocol

Solution. Next, we look at the Guillou-Quisquater (GQ) identification protocol with artificially created (small) parameters and $t = 1$.

1.
   - First, the authority T selects the primes $p = 569$ and $q = 739$ and calculates $n = pq = 420491$.
   - Next, T chooses the public exponent $v = 54955$ and calculates $\phi = (p-1)(q-1) = 419184$. Then it calculates its private exponent $s = v^{-1} \bmod \phi = 233875$.
   - The system parameters are (v, n), i.e. $(54955, 420491)$, are made available to all users.

Guillou-Quisquater (GQ) identification protocol

2. - Assume that the redundant identity of A is $J_A = 34579$.
   - Next, T gives A the secret $s_A = (J_A)^{-s} \bmod n = 403154$.
3. *Protocol messages.* Each of t rounds has three messages as follows.

$$A \rightarrow B : I_A,\ x = r^v \bmod n \qquad (1)$$

$$A \leftarrow B : e \text{ (where } 1 \leq e \leq v) \qquad (2)$$

$$A \rightarrow B : y = r \cdot {s_A}^e \bmod n \qquad (3)$$

Guillou-Quisquater (GQ) identification protocol

4.
- A chooses a random secret integer $r = 65446$ and calculates $x = r^v \bmod n = 89525$.
- A sends B a pair of integers $(I_A, 89525)$.
- B sends A a random integer (challenge) $e = 38980$.
- A calculates and sends B (answer) $y = r \cdot {s_A}^e \bmod n = 83551$.
- B computes $z = {J_A}^e \cdot y^v \bmod n = 89525$ and accepts an identity proof from A, because $z = x$.

Schnorr identification protocol

- Schnorr identification protocol is an alternative to the Fiat-Shamir and GQ protocols. Its security is based on the intractability of the discrete logarithm problem.
- The basic idea is that A proves knowledge of a secret a (without revealing it) in a time-variant manner (depending on a challenge e), identifying A through the association of a with the public key v via A's authenticated certificate.

Schnorr identification protocol

Algorithm 4 Schnorr identification protocol

SUMMARY. A proves its identity to B in a 3-pass protocol.

1. *Selection of system parameters.*
   - A suitable prime p is selected such that $p-1$ is divisible by another prime q. (Discrete logarithms modulo p must be computationally infeasible e.g., $p \approx 2^{1024}, q \geq 2^{160}$.)
   - An element β is chosen, $1 \leq \beta \leq p-1$, having multiplicative order q. (For example, for α generator mod $p, \beta = \alpha^{\frac{(p-1)}{q}}$ mod p.)
   - Each party obtains an authentic copy of the system parameters (p, q, β) and the verification function (public key) of the trusted party T, allowing verification of T's signatures $S_T(m)$ on messages m. (S_T involves a suitable known hash function prior to signing, and may be any signature mechanism.)
   - A parameter t (e.g.,$t \geq 40), 2^t < q$, is chosen (defining a security level 2^t).

Schnorr identification protocol

Algorithm 4 Schnorr identification protocol

2. *Selection of per-user parameters.*
   - Each entity A is given a unique identity I_A.
   - A chooses a private key $a, 0 \leq a \leq q-1$, and computes $v = \beta^{-a}$ mod p.
   - A identifies itself by conventional means (e.g., passport) to T, transfers v to T with integrity, and obtains a certificate $cert_A = (I_A, v, S_T(I_A, v))$ from T binding I_A with v.
3. *Protocol messages.* The protocol involves three messages.
   - $A \rightarrow B : cert_A,\ x = \beta^r$ mod p (2)
   - $A \leftarrow B : e$ (where $1 \leq e \leq 2^t < q$)
   - $A \rightarrow B : y = ae + r$ mod q

Schnorr identification protocol

Algorithm 4 Schnorr identification protocol

4. *Protocol actions.* A identifies itself to verifier B as follows.
   - A selects a random r(the commitment), $1 \leq r \leq q-1$, computes (the witness) $x = \beta^r$ mod p, and sends (2) to B.
   - B authenticates A's public key v by verifying T's signature on $cert_A$, then sends to A a (never previously used) random e (the challenge), $1 \leq e \leq 2^t$.
   - A checks $1 \leq e \leq 2^t$ and sends B (the response) $y = ae + r$ mod q.
   - B computes $z = \beta^y v^e$ mod p, and accepts A's identity provided $z = x$.

Schnorr identification protocol

Example. Consider a Schnorr identification protocol between Alice and Bob with primes $p = 48731$ and $q = 443$, $\alpha = 6$ and $t = 8$ and Alice's private key is $a = 357$. Describe the communication between Alice and By Bob if she chooses $r = 274$ and he challenges $e = 129$.

Solution. Let's look at Schnorr's identification protocol with artificially created (small) parameters from the example.

1.
   - First, the authority T selected a prime number $p = 48731$, where $p - 1$ is divisible by another prime number $q = 443$.
   - The generator mod 48731 is $\alpha = 6$ and β is calculated as $\beta = \alpha^{\frac{(p-1)}{q}} \bmod p = 11444$.
   - The system parameters are (p, q, β), i.e. $(48731, 443, 11444)$.
   - We choose $t = 8$.

Schnorr identification protocol

2. - A chooses the private key $a = 357$ and computes $v = \beta^{-a} \bmod p = 7355$.

3. *Protocol messages.* The protocol involves three messages.

$$A \rightarrow B : cert_A,\ x = \beta^r \bmod p \qquad (1)$$

$$A \leftarrow B : e\ (\text{ where } 1 \leq e \leq 2^t < q) \qquad (2)$$

$$A \rightarrow B : y = ae + r \bmod q \qquad (3)$$

Schnorr identification protocol

4.
- A picks a random $r = 274$ and calculates $x = \beta^r \bmod p = 37123$ and sends to user B.
- B sends A and a random challenge $e = 129$.
- A sends B (response) $y = ae + r \bmod q = 255$.
- B computes $z = \beta^y v^e \bmod p = 37123$ and accepts the identity of A provided that $z = x$.

Shamir's (t, n) Threshold Scheme

- In 1979, Israeli cryptanalyst Adi Shamir proposed a threshold scheme for sharing secrets between n parties that allows sharing in such a way that
  - t and more users are enough to restore the secret
  - of no $t-1$ or fewer users can obtain any secret information.
- The basic idea of Shamir's (t, n) thresholding scheme is that t points define a polynomial of degree $t-1$ (ie, 2 points are enough to define a straight line and 3 points to define a parabola, etc.).

Shamir's (t, n) Threshold Scheme

Example. In Shamir's $(3, 5)$ scheme for $p = 17$, Alice, Bob and Charles were given the following (x_i, y_i) values: $(1, 8), (3, 10), (5, 11)$. Compute the corresponding Lagrangian interpolation polynomial and determine the secret.

Shamir's Secret Sharing

Solution. Let's calculate the Lagrange interpolation polynomial using the following formulas:

$$F(x) = \sum_{i=1} y_i l_i(x) \mod p$$

$$l_i(x) = \prod_{j \neq i} \frac{x - x_j}{x_i - x_j} \mod p$$

$$l_1 = \frac{x-3}{1-3} \cdot \frac{x-5}{1-5} = \frac{x^2 - 8x + 15}{8} \mod 17$$

$$l_2 = \frac{x-1}{3-1} \cdot \frac{x-5}{3-5} = \frac{x^2 - 6x + 5}{-4} \mod 17$$

$$l_3 = \frac{x-1}{5-1} \cdot \frac{x-3}{5-3} = \frac{x^2 - 4x + 3}{8} \mod 17$$

Shamir's Secret Sharing

$$p(x) = \sum_{k=1}^{3} y_k l_k(x)$$

$$p(x) = 8 \cdot \frac{x^2 - 8x + 15}{8} + 10 \cdot \frac{x^2 - 6x + 5}{-4} + 11 \cdot \frac{x^2 - 4x + 3}{8}$$

$$\begin{aligned} p(x) &= \frac{1}{8}(8x^2 - 64x + 120 - 20x^2 + 120x - 100 + 11x^2 - 44x + 33) \\ &= \frac{1}{8}(-x^2 + 12x + 53) \\ &= 15(-x^2 + 12x + 53) \\ &= (-15x^2 + 180x + 795) \\ &= 2x^2 + 10x + 13 \mod 17 \end{aligned}$$

Shamir's Secret Sharing

Finally we have the following polynomial

$$p(x) = 2x^2 + 10x + 13 \mod 17,$$

then the secret is 13.

Shamir's Secret Sharing

Example. You need to set up a Shamir $(2, 30)$ scheme for $p = 101$. Alice and Bob shared the following values: $(1, 13)$ and $(3, 12)$. Another person received $(2, *)$, but the part marked $*$ is unreadable. What is the correct value of $*$?

Shamir's Secret Sharing

Solution. Consider a polynomial in the general form $ax + b \mod 101$. The polynomial has degree 1. We need 2 values to find the secret of b. We substitute the known values of Alice and Bob and get:

$$b + a = 13 \mod 101$$

$$b + 3a = 12 \mod 101.$$

Written in matrix form

$$\begin{pmatrix} 1 & 1 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} b \\ a \end{pmatrix} = \begin{pmatrix} 13 \\ 12 \end{pmatrix} \mod 101$$

The solution is:

$$\begin{pmatrix} b \\ a \end{pmatrix} = \begin{pmatrix} \frac{27}{2} \\ \frac{-1}{2} \end{pmatrix} \mod 101$$

Shamir's Secret Sharing

We know, that $\frac{1}{2} = 51 \mod 101$. Then

$b = 27 \cdot (\frac{1}{2}) \mod 101 = 27 \cdot (51) \mod 101 = 64 \mod 101$.

Similarly,

$$a = -51 \mod 101.$$

We have the following polynomial:

$$64 - 51x \mod 101.$$

The third value is then the evaluation of this polynomial at $x = 2$, which is 63.

Shamir's Secret Sharing

Example. There are four people in the room and we know that exactly one of them is a spy. The other three people share secrets using Shamir's (2,3) scheme over $\mathbb{Z}_{11}$. The spy randomly chose his share. The four pairs are $P_1 = (1, 7), P_2 = (3, 0), P_3 = (5, 10)$ a $P_4 = (7, 9)$. Find out which pair was created by a spy.

Solution. The indicated shares correspond to the following equations (for the polynomial $ax + b$):

$$7 = a + b \mod 11$$
$$0 = 3a + b \mod 11$$
$$10 = 5a + b \mod 11$$
$$9 = 7a + b \mod 11$$

From the first two equations we have $a = 2$ and $b = 5$, but this solution does not apply to the third and fourth equations. Therefore, the spy must be either a person with P_1 or P_2. We further see that from the first and third equations we have $a = 9$ and $b = 9$. Further, we see that this solution does not apply to the fourth equation. Therefore, a spy is a person with a share of P_1.