Excursion: some basic properties of numbers

$gcd(a,b)$ (also written (a,b)) can be computed by the Euclid's algorithm.

$$\text{gcd (a,b)} = \text{gcd (b,a} \mod \text{b)}$$

$gcd(56,21)$

$= gcd(21,14) \qquad // \ 14 = 1 \times 56 - 2 \times 21$

$= gcd(14,7) \qquad // \ 7 = 1 \times 21 - 1 \times 14$

$= 7 \qquad // \ 14 \bmod 7 = 0$

Excursion: some basic properties of numbers

$gcd(a, b)$ (also written (a, b)) can be computed by the Euclid's algorithm.

$$\text{gcd (a,b)} = \text{gcd (b,a} \mod \text{b)}$$

$$\begin{aligned}
& gcd(56, 21) \\
& = gcd(21, 14) && // \ 14 = 1 \times 56 - 2 \times 21 \\
& = gcd(14, 7) && // \ 7 = 1 \times 21 - 1 \times 14 \\
& = 7 && // \ 14 \bmod 7 = 0
\end{aligned}$$

$$7 = 1 \times 21 - 1 \times 14 = 1 \times 21 - (1 \times 56 - 2 \times 21) = -1 \times 56 + 3 \times 21$$

Excursion: some basic properties of numbers

$gcd(a, b)$ (also written (a, b)) can be computed by the Euclid's algorithm.

$$\text{gcd (a,b)} = \text{gcd (b,a} \mod \text{b)}$$

$$\begin{aligned}
& gcd(56, 21) \\
& = gcd(21, 14) && // \ 14 = 1 \times 56 - 2 \times 21 \\
& = gcd(14, 7) && // \ 7 = 1 \times 21 - 1 \times 14 \\
& = 7 && // \ 14 \text{ mod } 7 = 0
\end{aligned}$$

$$7 = 1 \times 21 - 1 \times 14 = 1 \times 21 - (1 \times 56 - 2 \times 21) = -1 \times 56 + 3 \times 21$$

$\Rightarrow$ $gcd(a, b)$ is always of the form $ma + nb$ for some $m, n \in \mathbb{Z}$

Hence if $(a, b) = 1$ then $ma + nb = 1$ for some $m, n \in \mathbb{Z}$.

Conversely suppose $ma + nb = 1$.

Let k be a common divisor of a and b.

We have $a = uk$ and $b = vk$.

Then $1 = ma + nb = k(mu + nv)$.

This is possible only if $k = 1$.

Conclusion: $(a, b) = 1$ if and only if $ma + nb = 1$ for some $m, n \in \mathbb{Z}$.

For any $p \in \mathbb{N}$, consider $\mathbb{Z}_p^* = \{x \mid 0 < x < p, (x,p) = 1\}$, and the operation of multiplication modulo p.

Let $x, y \in \mathbb{Z}_p^*$.

We have $mx + np = 1$ and $m'y + n'p = 1$.

$$mm'xy = 1 - np - n'p + nn'p^2$$
$$mm'xy + (n + n' - nn'p)p = 1$$

$(xy, p) = 1$. Hence $(xy \bmod p, p) = 1$.

Conclusion: if $x, y \in \mathbb{Z}_p^*$ then $xy \bmod p \in \mathbb{Z}_p^*$.

For any $p \in \mathbb{N}$, consider $\mathbb{Z}_p^* = \{x \mid 0 < x < p, (x, p) = 1\}$, and the operation of multiplication modulo p.

Let $x, y \in \mathbb{Z}_p^*$.

We have $mx + np = 1$ and $m'y + n'p = 1$.

$$mm'xy = 1 - np - n'p + nn'p^2$$
$$mm'xy + (n + n' - nn'p)p = 1$$

$(xy, p) = 1$. Hence $(xy \bmod p, p) = 1$.

Conclusion: if $x, y \in \mathbb{Z}_p^*$ then $xy \bmod p \in \mathbb{Z}_p^*$.

Also we have $mx \bmod p = 1$.

Conclusion: for every $x \in \mathbb{Z}_p^*$ there is some $x^{-1} \in \mathbb{Z}_p^*$ such that $xx^{-1} \bmod p = 1$.

Hence the set $\mathbb{Z}_p^*$ with the operation of multiplication modulo p forms a group, i.e. a set G with a binary operation $\times$ such that

1. if $x, y \in G$ then $x \times y \in G$
2. associativity: $(x \times y) \times z = x \times (y \times z)$
3. identity element: there is an $e \in G$ such that $e \times x = x \times e = e$.
4. inverse elements: for every $x \in G$ there is some $x^{-1} \in G$ such that $x \times x^{-1} = x^{-1} \times x = e$.

Hence the set $\mathbb{Z}_p^*$ with the operation of multiplication modulo p forms a group, i.e. a set G with a binary operation $\times$ such that

1. if $x, y \in G$ then $x \times y \in G$
2. associativity: $(x \times y) \times z = x \times (y \times z)$
3. identity element: there is an $e \in G$ such that $e \times x = x \times e = e$.
4. inverse elements: for every $x \in G$ there is some $x^{-1} \in G$ such that $x \times x^{-1} = x^{-1} \times x = e$.

In our case we have

$$G \equiv \mathbb{Z}_p^*$$
$$x \times y \equiv xy \bmod p$$
$$e \equiv 1$$

Examples of infinite groups

- integers with addition operation

$$x + 0 = 0 + x = x$$
$$x + (-x) = 0$$

- non-zero reals with multiplication operation

$$x \times 1 = 1 \times x = x$$
$$x \times (\frac{1}{x}) = 1$$

Example of a finite group: Booleans with exclusive-or operation

$$x \oplus 0 = 0 \oplus x = x$$
$$x + x = 0$$

Each element is its own inverse.

Observe: the group has 2 elements and also $x^2 = 0$ for all x.

Another finite group $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$

$2 \times 2 = 4 \quad 2 \times 3 = 1 \quad 2 \times 4 = 3 \quad 3 \times 3 = 4 \quad 3 \times 4 = 2 \quad 4 \times 4 = 1$

We have $\quad 1^{-1} = 1 \quad 2^{-1} = 3 \quad 3^{-1} = 2 \quad 4^{-1} = 4$

Another finite group $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$

$2 \times 2 = 4 \quad 2 \times 3 = 1 \quad 2 \times 4 = 3 \quad 3 \times 3 = 4 \quad 3 \times 4 = 2 \quad 4 \times 4 = 1$

We have $\quad 1^{-1} = 1 \quad 2^{-1} = 3 \quad 3^{-1} = 2 \quad 4^{-1} = 4$

Also $\quad 2^0 = 1 \quad 2^1 = 2 \quad 2^2 = 4 \quad 2^3 = 3$

Hence 2 is a generator of the group.

Another finite group $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$

$2 \times 2 = 4 \quad 2 \times 3 = 1 \quad 2 \times 4 = 3 \quad 3 \times 3 = 4 \quad 3 \times 4 = 2 \quad 4 \times 4 = 1$

We have $\quad 1^{-1} = 1 \quad 2^{-1} = 3 \quad 3^{-1} = 2 \quad 4^{-1} = 4$

Also $\quad 2^0 = 1 \quad 2^1 = 2 \quad 2^2 = 4 \quad 2^3 = 3$

Hence 2 is a generator of the group.

Similarly $\quad 3^0 = 1 \quad 3^1 = 3 \quad 3^2 = 4 \quad 3^3 = 2$

Hence 3 is also a generator of the group.

Another finite group $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$

$2 \times 2 = 4 \quad 2 \times 3 = 1 \quad 2 \times 4 = 3 \quad 3 \times 3 = 4 \quad 3 \times 4 = 2 \quad 4 \times 4 = 1$

We have $\quad 1^{-1} = 1 \quad 2^{-1} = 3 \quad 3^{-1} = 2 \quad 4^{-1} = 4$

Also $\quad 2^0 = 1 \quad 2^1 = 2 \quad 2^2 = 4 \quad 2^3 = 3$

Hence 2 is a generator of the group.

Similarly $\quad 3^0 = 1 \quad 3^1 = 3 \quad 3^2 = 4 \quad 3^3 = 2$

Hence 3 is also a generator of the group.

$\phi(5) = |\mathbb{Z}_5^*| = 4$ (The familiar Euler phi function)

Observe $\quad 1^4 = 1 \quad 2^4 = 1 \quad 3^4 = 1 \quad 4^4 = 1$

Another finite group $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$

$2 \times 2 = 4 \quad 2 \times 3 = 1 \quad 2 \times 4 = 3 \quad 3 \times 3 = 4 \quad 3 \times 4 = 2 \quad 4 \times 4 = 1$

We have $\quad 1^{-1} = 1 \quad 2^{-1} = 3 \quad 3^{-1} = 2 \quad 4^{-1} = 4$

Also $\quad 2^0 = 1 \quad 2^1 = 2 \quad 2^2 = 4 \quad 2^3 = 3$

Hence 2 is a generator of the group.

Similarly $\quad 3^0 = 1 \quad 3^1 = 3 \quad 3^2 = 4 \quad 3^3 = 2$

Hence 3 is also a generator of the group.

$\phi(5) = |\mathbb{Z}_5^*| = 4$ (The familiar Euler phi function)

Observe $\quad 1^4 = 1 \quad 2^4 = 1 \quad 3^4 = 1 \quad 4^4 = 1$

But also $4^2 = 1$.

The set $\{1, 4\}$ is also a group wrt multiplication modulo 5.

Hence $\{1, 4\}$ is a subgroup of $\mathbb{Z}_5^*$ and $|\{1, 4\}| = 2$.

$\mathbb{Z}_8^* = \{1, 3, 5, 7\}$

$3 \times 3 = 1 \quad 3 \times 5 = 7 \quad 3 \times 7 = 5 \quad 5 \times 5 = 1 \quad 5 \times 7 = 3 \quad 7 \times 7 = 1$

We have $\quad 1^{-1} = 1 \quad 3^{-1} = 3 \quad 5^{-1} = 5 \quad 7^{-1} = 7$

$\mathbb{Z}_8^* = \{1, 3, 5, 7\}$

$3 \times 3 = 1 \quad 3 \times 5 = 7 \quad 3 \times 7 = 5 \quad 5 \times 5 = 1 \quad 5 \times 7 = 3 \quad 7 \times 7 = 1$

We have $\quad 1^{-1} = 1 \quad 3^{-1} = 3 \quad 5^{-1} = 5 \quad 7^{-1} = 7$

Also $\quad 3^0 = 1 \quad 3^1 = 3 \quad 3^2 = 1$

$\mathbb{Z}_8^* = \{1, 3, 5, 7\}$

$3 \times 3 = 1 \quad 3 \times 5 = 7 \quad 3 \times 7 = 5 \quad 5 \times 5 = 1 \quad 5 \times 7 = 3 \quad 7 \times 7 = 1$

We have $1^{-1} = 1 \quad 3^{-1} = 3 \quad 5^{-1} = 5 \quad 7^{-1} = 7$

Also $3^0 = 1 \quad 3^1 = 3 \quad 3^2 = 1$

Similarly $5^0 = 1 \quad 5^1 = 5 \quad 5^2 = 1$

And $7^0 = 1 \quad 7^1 = 7 \quad 7^2 = 1$

$\mathbb{Z}_8^* = \{1, 3, 5, 7\}$

$3 \times 3 = 1 \quad 3 \times 5 = 7 \quad 3 \times 7 = 5 \quad 5 \times 5 = 1 \quad 5 \times 7 = 3 \quad 7 \times 7 = 1$

We have $1^{-1} = 1 \quad 3^{-1} = 3 \quad 5^{-1} = 5 \quad 7^{-1} = 7$

Also $3^0 = 1 \quad 3^1 = 3 \quad 3^2 = 1$

Similarly $5^0 = 1 \quad 5^1 = 5 \quad 5^2 = 1$

And $7^0 = 1 \quad 7^1 = 7 \quad 7^2 = 1$

$\phi(8) = |\mathbb{Z}_5^*| = 4$

Observe $1^4 = 1 \quad 3^4 = 1 \quad 5^4 = 1 \quad 7^4 = 1$

$\mathbb{Z}_8^* = \{1, 3, 5, 7\}$

$3 \times 3 = 1 \quad 3 \times 5 = 7 \quad 3 \times 7 = 5 \quad 5 \times 5 = 1 \quad 5 \times 7 = 3 \quad 7 \times 7 = 1$

We have $\quad 1^{-1} = 1 \quad 3^{-1} = 3 \quad 5^{-1} = 5 \quad 7^{-1} = 7$

Also $\quad 3^0 = 1 \quad 3^1 = 3 \quad 3^2 = 1$

Similarly $\quad 5^0 = 1 \quad 5^1 = 5 \quad 5^2 = 1$

And $\quad 7^0 = 1 \quad 7^1 = 7 \quad 7^2 = 1$

$\phi(8) = |\mathbb{Z}_5^*| = 4$

Observe $\quad 1^4 = 1 \quad 3^4 = 1 \quad 5^4 = 1 \quad 7^4 = 1$

But also $3^2 = 5^2 = 7^2 = 1$.

The sets $\{1, 3\}, \{1, 5\}, \{1, 7\}$ are each groups wrt multiplication modulo 8. Hence they are subgroups of $\mathbb{Z}_8^*$, each of order 2.

Consider a group G wrt the operation $\times$.

If $S \subseteq G$ and S is also a group wrt the same operation $\times$, then S is called a subgroup of G.

Consider a group G wrt the operation $\times$.

If $S \subseteq G$ and S is also a group wrt the same operation $\times$, then S is called a subgroup of G.

Fact: if S is a subgroup of a finite group G then $|S|$ divides $|G|$.

Consider a group G wrt the operation $\times$.

If $S \subseteq G$ and S is also a group wrt the same operation $\times$, then S is called a subgroup of G.

Fact: if S is a subgroup of a finite group G then $|S|$ divides $|G|$.

Fact: if G is a finite group and $x \in G$ then $x^{|G|} = e$.

Consider a group G wrt the operation $\times$.

If $S \subseteq G$ and S is also a group wrt the same operation $\times$, then S is called a subgroup of G.

Fact: if S is a subgroup of a finite group G then $|S|$ divides $|G|$.

Fact: if G is a finite group and $x \in G$ then $x^{|G|} = e$.

Hence if $x \in \mathbb{Z}_p^*$ then $x^{\phi(p)} = 1$
(mod p of course, but this is often left unwritten)

We used this for our discussion on RSA. Recall:

$\phi(p) = \mathbb{Z}_p^* = |\{1, \ldots, p-1\}| = p - 1$ when p is prime.

$\phi(pq) = \mathbb{Z}_{pq}^* = |\{1, \ldots, pq-1\} \setminus \{p, 2p, \ldots, (q-1)p, q, 2q, \ldots, (p-1)q\}|$
$= pq - 1 - (p - 1 + q - 1) = (p-1)(q-1)$ when p and q are distinct primes.

Let G be a group and $a \in G$.
Consider the set $\langle a \rangle = \{a^i \mid i \in \mathbb{Z}\} \subseteq G$.
(a^3 denotes $a \times a \times a$; a^0 denotes e; a^{-3} denotes $(a^{-1})^3$)

Clearly $\langle a \rangle$ is a subgroup of G:

- Take any two elements a^i and a^j from $\langle a \rangle$. Then $a^i \times a^j = a^{i+j} \in \langle a \rangle$.
- Associativity property holds already for the whole group G.
- $e = a^0 \in \langle a \rangle$.
- Take any element $a^i \in \langle a \rangle$. Then we know that $a^i \times a^{-i} = (a \times a^{-1})^i = e^i = e$ and $a^{-i} \in \langle a \rangle$. Also $a^{-i} \times a^i = e$.

$\langle a \rangle$ is called the subgroup generated by a.
Further if $\langle a \rangle = G$ then a is called a generator of G, and G is called a cyclic group.

In case of the groups $\mathbb{Z}_p^*$ we know that $x^{\phi(p)} = 1$ for every $x \in \mathbb{Z}_p^*$.

Hence it is unnecessary to consider negative powers.

$x^{-1} = x^{-1}x^{\phi(p)} = x^{\phi(p)-1}, \qquad x^{-2} = (x^{-1})^2 \ldots.$

Hence $\langle x \rangle = \{x^0, x^1, x^2 \ldots\}$

Also $x^{\phi(p)} = x^0, \quad x^{\phi(p)+1} = x^1 \ldots$

Hence $\langle x \rangle = \{x^0, x^1, x^2 \ldots, x^{\phi(p)-1}\}$

For the group $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$ we have

$\langle 1 \rangle = \{1\} \qquad \langle 2 \rangle = \{1, 2, 4, 3\} \qquad \langle 3 \rangle = \{1, 3, 4, 2\} \qquad \langle 4 \rangle = \{1, 4\}$

$\mathbb{Z}_5^*$ is cyclic because it has generators 2 and 3.

$\mathbb{Z}_8^*$ is not cyclic: $\langle 3 \rangle = \{1, 3\}, \qquad \langle 5 \rangle = \{1, 5\}, \qquad \langle 7 \rangle = \{1, 7\}$

In case of the groups $\mathbb{Z}_p^*$ we know that $x^{\phi(p)} = 1$ for every $x \in \mathbb{Z}_p^*$.

Hence it is unnecessary to consider negative powers.

$x^{-1} = x^{-1}x^{\phi(p)} = x^{\phi(p)-1}, \qquad x^{-2} = (x^{-1})^2 \ldots.$

Hence $\langle x \rangle = \{x^0, x^1, x^2 \ldots\}$

Also $x^{\phi(p)} = x^0, \quad x^{\phi(p)+1} = x^1 \ldots$

Hence $\langle x \rangle = \{x^0, x^1, x^2 \ldots, x^{\phi(p)-1}\}$

For the group $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$ we have

$\langle 1 \rangle = \{1\} \qquad \langle 2 \rangle = \{1, 2, 4, 3\} \qquad \langle 3 \rangle = \{1, 3, 4, 2\} \qquad \langle 4 \rangle = \{1, 4\}$

$\mathbb{Z}_5^*$ is cyclic because it has generators 2 and 3.

$\mathbb{Z}_8^*$ is not cyclic: $\langle 3 \rangle = \{1, 3\}, \qquad \langle 5 \rangle = \{1, 5\}, \qquad \langle 7 \rangle = \{1, 7\}$

Fact: $\mathbb{Z}_p^*$ is cyclic for every prime p.

Back to the Diffie-Hellman secret key exchange

p is a prime and g is a generator of $\mathbb{Z}_p^*$.

A and B choose randomly N_a and N_b respectively from $\{0, 1, \ldots, p-2\}$ and exchange the messages g^{N_a} and g^{N_b}.

The common key computed by both is $g^{N_a N_b}$.

The exchanged messages and the common keys are all from the set $\mathbb{Z}_p^*$.

The recommended size of p is 512 bits or better 1024 bits.

Back to the Diffie-Hellman secret key exchange

p is a prime and g is a generator of $\mathbb{Z}_p^*$.

A and B choose randomly N_a and N_b respectively from $\{0, 1, \ldots, p-2\}$ and exchange the messages g^{N_a} and g^{N_b}.

The common key computed by both is $g^{N_a N_b}$.

The exchanged messages and the common keys are all from the set $\mathbb{Z}_p^*$.

The recommended size of p is 512 bits or better 1024 bits.

How secure is this protocol?

Important: this protocol should not be analyzed according to the usual Dolev-Yao model.

E.g. suppose we model message x^y as the term $exp(x, y)$.

The key computed by A is then $exp(exp(g, N_b), N_a)$
and that computed by B is $exp(exp(g, N_a), N_b)$.

But in the Dolev-Yao model, distinct terms represent distinct messages.

Hence in the normal run of the protocol (without interference from the attacker), the keys computed by A and B are not the same!

A possible solution: consider extensions of the Dolev-Yao model with certain equations on terms, e.g. $exp(exp(x, y), z) = exp(exp(x, z), y)$ . . .

The protocol provides no authentication.

An attack: attacker C pretends to be A, starts a session with B and computes a common key.

The protocol provides no authentication.

An attack: attacker C pretends to be A, starts a session with B and computes a common key.

Another attack, A may send g^{N_a} to B which is intercepted by C who replies with his own message g^{N_c}.
A thinks he has a common key $g^{N_a N_c}$ with B
but actually the key is known to C.

The protocol provides no authentication.

An attack: attacker C pretends to be A, starts a session with B and computes a common key.

Another attack, A may send g^{N_a} to B which is intercepted by C who replies with his own message g^{N_c}.
A thinks he has a common key $g^{N_a N_c}$ with B
but actually the key is known to C.

The protocol is clearly insecure in the presence of an active attacker.

We now consider a passive adversary: one who spies on messages in the network but does not modify them.

The passive adversary observes the messages g^{N_a} and g^{N_b}.
Also the values p and g are public.

Can the intruder compute the common key $g^{N_a N_b}$ from them.

The passive adversary observes the messages g^{N_a} and g^{N_b}.
Also the values p and g are public.

Can the intruder compute the common key $g^{N_a N_b}$ from them.

A suggestion: from g^{N_a} the attacker computes N_a, and from g^{N_b} he computes N_b. From these he can easily compute $g^{N_a N_b}$.

The passive adversary observes the messages g^{N_a} and g^{N_b}.
Also the values p and g are public.

Can the intruder compute the common key $g^{N_a N_b}$ from them.

A suggestion: from g^{N_a} the attacker computes N_a, and from g^{N_b} he computes N_b. From these he can easily compute $g^{N_a N_b}$.

The discrete logarithm problem: given a prime p,
a generator g of the group $\mathbb{Z}_p^*$ and an element $M \in \mathbb{Z}_p^*$,
compute the unique $x \in \{0, \ldots, p-2\}$ such that $g^x \bmod p = M$

The passive adversary observes the messages g^{N_a} and g^{N_b}.
Also the values p and g are public.

Can the intruder compute the common key $g^{N_a N_b}$ from them.

A suggestion: from g^{N_a} the attacker computes N_a, and from g^{N_b} he computes N_b. From these he can easily compute $g^{N_a N_b}$.

The discrete logarithm problem: given a prime p,
a generator g of the group $\mathbb{Z}_p^*$ and an element $M \in \mathbb{Z}_p^*$,
compute the unique $x \in \{0, \ldots, p-2\}$ such that $g^x \bmod p = M$

A naive algorithm: for each $x \in \{0, \ldots, p-2\}$ check whether
$g^x \bmod p = M$.

The number of possibilities for x is exponential
in the binary representation of p.

One-way functions are functions f such that it is "easy" to compute $f(x)$ from x but "difficult" to compute x from $f(x)$.

The function f where $f(p, g, x) = g^x \bmod p$ is believed to be one-way, but no proof is known.

I.e. the discrete logarithm problem is believed to be difficult.

The Diffie-Hellman problem: Given g^x and g^y for some x, y chosen from $\{0, \ldots, p-2\}$, compute g^{xy}.

The discrete logarithm problem is at least as difficult as the Diffie-Hellman problem, i.e. solving the former allows one to solve the latter.

The converse is an open question: does solving the Diffie-Hellman problem allow us to solve the discrete logarithm problem?

The Diffie-Hellman assumption: The Diffie-Hellman problem is difficult.

In fact it is unknown whether there are any one-way functions at all!

Some other functions which are believed to be one-way:

- Factoring. The function $f(x, y) = xy$ is believed to be one-way.
- RSA. The function is $f(x) = x^e \bmod n$ where $n = pq$ for two primes p, q with $(e, \phi(n)) = 1$.
  This is believed to be a trapdoor one-way function with secrets p, q: knowledge of the secrets allows one to invert f, but inverting f is difficult otherwise.
  The best known algorithm for inverting f is to factor N.

In fact it is unknown whether there are any one-way functions at all!

Some other functions which are believed to be one-way:

- Factoring. The function $f(x, y) = xy$ is believed to be one-way.
- RSA. The function is $f(x) = x^e \bmod n$ where $n = pq$ for two primes p, q with $(e, \phi(n)) = 1$.
  This is believed to be a trapdoor one-way function with secrets p, q: knowledge of the secrets allows one to invert f, but inverting f is difficult otherwise.
  The best known algorithm for inverting f is to factor N.

Summary: The Diffie-Hellman secret key exchange protocol is secure in the presence of a passive attacker (under the DH assumption)

Key distribution in the two-party symmetric key model

The two parties already share a (symmetric) long-lived key and want to compute a common symmetric key for a session.

No trusted third party is involved.

Possible motivations:

– prevent over-exposure of and repeated access to the long lived key.

– another motivation, especially in the asymmetric key model (where the long lived keys are asymmetric), is that symmetric key cryptography is much more efficient.

A message authentication scheme consists of a tagging algorithm $\mathcal{T}$ and a verification algorithm $\mathcal{V}$.

Given a message m and a key K we can compute the tag

$$t = \mathcal{T}_K(m) \quad .$$

A person knowing m and K can then verify the tag.

$$b = \mathcal{V}_K(m, t) \quad .$$

We require the property

$$\mathcal{V}_K(m, \mathcal{T}_K(m)) = 1$$

Security requirement: it is difficult for an attacker to forge a pair m, t such that $\mathcal{V}_K(m, t) = 1$.

I.e. the attacker tries to produce a tag for a new message after having observed some tags of other messages.

The AKEP1 protocol (Authenticated Key Exchange Protocol 1)

A and B share a long-lived key K^e_{ab} for symmetric encryption and a long-lived key K^m_{ab} for message authentication.

$$
\begin{aligned}
A \to B: &\quad A, N_a \\
B \to A: &\quad N_b, \{k\}_{K^e_{ab}}, \mathcal{T}_{K^m_{ab}}(\langle B, A, N_a, N_b, \{k\}_{K^e_{ab}} \rangle) \\
A \to B: &\quad \mathcal{T}_{K^m_{ab}}(\langle A, N_b \rangle)
\end{aligned}
$$

N_a and N_b are nonces generated by A and B respectively.
k is the session key (nonce) generated by B.

A and B first verify that the respective tags they received are correct, before accepting the session key.

Informal analysis.

$$\begin{aligned} A \to B: &\quad A, N_a \\ B \to A: &\quad N_b, \{k\}_{K_{ab}^e}, \mathcal{T}_{K_{ab}^m}(\langle B, A, N_a, N_b, \{k\}_{K_{ab}^e}\rangle) \\ A \to B: &\quad \mathcal{T}_{K_{ab}^m}(\langle A, N_b\rangle) \end{aligned}$$

From point of view of A:

If A and B are honest then K_{ab}^e and K_{ab}^m are known only to A and B. Hence the encryption $\{k\}_{K_{ab}^e}$ must have been performed by B.

The tag he receives must have been created by B. Hence the encryption $\{k\}_{K_{ab}^e}$ was performed by B in response to the nonce N_a that he sent.

From point of view of B: the tag he receives ensures that the tag in the second step was accepted by A.

The two-party asymmetric model

A digital signature scheme consists of a signing algorithm $\mathcal{S}$ and a verification algorithm $\mathcal{V}$.

Given message m and private key K^{-1} we can compute the signature

$$s = \mathcal{S}_(K^{-1}, m) \qquad .$$

A person knowing m and K can then verify the signature.

$$b = \mathcal{V}(K, m, s) \qquad .$$

We require the property

$$\mathcal{V}(K, m, s) = 1 \text{ if and only if } s = \mathcal{S}(K^{-1}, m)$$

Security requirement: it is difficult for an attacker to forge a pair m, s such that $\mathcal{V}(K, m, s) = 1$.

The protocol

Each user A has public keys K_a^e and K_a^d for encryption and signature schemes respectively. The corresponding private keys are $K_a^{e^{-1}}$ and $K_a^{d^{-1}}$. These are long-lived keys. The symmetric session key k is created as:

$$
\begin{aligned}
A \to B: &\quad A, N_a \\
B \to A: &\quad N_b, \{k\}_{K_a^e}, \mathcal{S}(K_b^{d^{-1}}, \langle B, A, N_a, N_b, \{k\}_{K_{ab}^e} \rangle) \\
A \to B: &\quad \mathcal{S}(K_a^{d^{-1}}, \langle A, N_b \rangle)
\end{aligned}
$$

The protocol

Each user A has public keys K_a^e and K_a^d for encryption and signature schemes respectively. The corresponding private keys are $K_a^{e^{-1}}$ and $K_a^{d^{-1}}$. These are long-lived keys. The symmetric session key k is created as:

$$
\begin{aligned}
A \to B: &\quad A, N_a \\
B \to A: &\quad N_b, \{k\}_{K_a^e}, \mathcal{S}(K_b^{d^{-1}}, \langle B, A, N_a, N_b, \{k\}_{K_{ab}^e} \rangle) \\
A \to B: &\quad \mathcal{S}(K_a^{d^{-1}}, \langle A, N_b \rangle)
\end{aligned}
$$

Compare with the Needham-Schroeder public key protocol

$$
\begin{aligned}
A \longrightarrow B: &\quad \{A, N_a\}_{K_b^e} \\
B \longrightarrow A: &\quad \{N_a, N_b\}_{K_a^e} \\
A \longrightarrow B: &\quad \{N_b\}_{K_b^e}
\end{aligned}
$$

There B has no guarantee about who created the first and third messages.