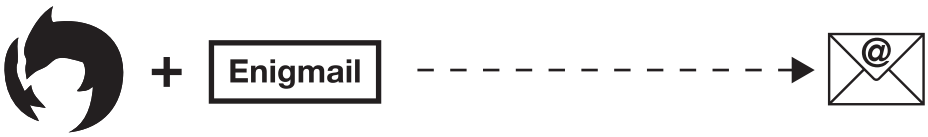
ZACZNIJ SZYFROWAĆ SWOJĄ POCZTĘ

PGP (czyli *Pretty Good Privacy*) oraz GPG (*GNU Privacy Guard*) to rozwiązania pozwalające na podpisywanie Twoich wiadomości w zaufany sposób (aby każdy mógł sprawdzić, czy to na pewno Ty je wysyłasz) i szyfrowanie ich, tak aby były czytelne tylko dla Ciebie i odbiorcy maila. Dzięki temu możesz zabezpieczyć swoją korespondencję przed „okiem" pośredników (np. Twojego operatora telekomunikacyjnego lub dostawca poczty), instytucji publicznych oraz innych osób, które mogą być zainteresowane jej treścią.

PANOPTYKON.ORG

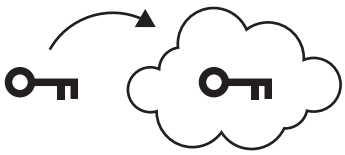
1. Będziesz potrzebować programu pocztowego, który obsługuje szyfrowanie – najpopularniejszym jest Mozilla Thunderbird z dodatkiem Enigmail. Możesz pobrać go za darmo z sieci.



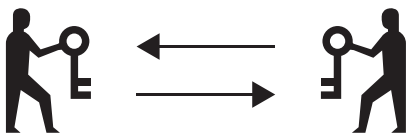
2. Podłącz do programu swoją skrzynkę pocztową. Te popularne (takie jak Gmail czy Yahoo) zrobią to prawie automatycznie.

3. Za pomocą wtyczki Enigmail wygeneruj tzw. parę kluczy. Publiczny będzie służył innym osobom do szyfrowania poczty wysyłanej do Ciebie, natomiast powiązany z nim prywatny klucz, zabezpieczony Twoim hasłem, ich odszyfrowywaniu.

4. Publiczny klucz wyślij na serwer kluczy (np. za pośrednictwem programu pocztowego), możesz go też załączać do Twoich maili. Dzięki niemu będzie można zweryfikować Ciebie jako nadawcę wiadomości.



5. Wymień się kluczami publicznymi z osobami, z którymi chcesz się bezpiecznie komunikować w Internecie.



6. Aby zaszyfrować treść wysyłanych przez siebie wiadomości, używaj kluczy publicznych Twoich odbiorców (nigdy swojego).

7. Teraz możesz komunikować się bezpiecznie, pamiętaj jednak, by zawsze zweryfikować klucz osoby, z którą korespondujesz!

8. Kiedy zweryfikujesz czyjś klucz, możesz potwierdzić wirtualną tożsamość tej osoby powiązaną z jej mailem. W ten sposób rozwijasz sieć zaufania (*web of trust*).