Szyfrowanie

Podstawy kryptografii w 12 min.

Szyfr - funkcja matematyczna wykorzystywana do szyfrowania tekstu jawnego lub jego deszyfrowania. Zazwyczaj jedna funkcja wykorzystywana jest do szyfrowania, a inna do deszyfrowania wiadomości. Wiadomość przed zaszyfrowaniem nazywana jest tekstem jawnym, zaś wiadomość zaszyfrowaną nazywamy szyfrogramem. Proces zamiany tekstu jawnego na szyfrogram nazywamy szyfrowaniem.

Co to jest szyfrowanie?

Szyfrowanie jest sposobem zapisu danych, aby tylko autoryzowane strony mogły zrozumieć informacje. Pod względem technicznym jest to proces przekształcania czytelnego dla człowieka tekstu jawnego w niezrozumiały tekst, znany również jako tekst szyfrowy. Mówiąc prościej, szyfrowanie pobiera czytelne Dane i zmienia je tak, że wydaje się losowe. Szyfrowanie wymaga użycia klucza kryptograficznego: zestawu wartości matematycznych, na które zgadzają się zarówno nadawca, jak i odbiorca zaszyfrowanej wiadomości., chociaż zaszyfrowane dane wydają się losowe, szyfrowanie przebiega w logiczny, przewidywalny sposób, pozwalając stronie, która otrzymuje zaszyfrowane dane i posiada odpowiedni klucz, aby odszyfrować dane, zamieniając je z powrotem w zwykły tekst. Prawdziwie bezpieczne szyfrowanie będzie używać kluczy na tyle skomplikowanych, że osoby trzecie raczej nie odszyfrowałyby lub złamałyby szyfrogramu za pomocą brutalnej siły - innymi słowy, zgadując klucz.

Dane mogą być szyfrowane „w spoczynku”, gdy są przechowywane lub „w tranzycie”, gdy są przesyłane gdzie indziej.

Co to jest klucz w kryptografii?

klucz kryptograficzny to ciąg znaków używany w algorytmie szyfrowania do zmiany danych tak, aby wyglądały one losowo. Podobnie jak klucz fizyczny, blokuje (szyfruje) dane tak, że tylko ktoś z odpowiednim kluczem może je odblokować (odszyfrować).

Jakie są różne rodzaje szyfrowania?

dwa główne rodzaje szyfrowania to szyfrowanie symetryczne i szyfrowanie asymetryczne. Szyfrowanie asymetryczne jest również znane jako szyfrowanie klucza publicznego.

W szyfrowaniu symetrycznym istnieje tylko jeden klucz, a wszystkie komunikujące się strony używają tego samego (tajnego) klucza zarówno do szyfrowania, jak i odszyfrowywania.,

W szyfrowaniu asymetrycznym lub publicznym istnieją dwa klucze: jeden klucz jest używany do szyfrowania, a inny klucz jest używany do deszyfrowania. Klucz deszyfrujący jest przechowywany jako prywatny (stąd nazwa „klucz prywatny”), podczas gdy klucz szyfrujący jest udostępniany

publicznie, dla każdego (stąd nazwa „klucz publiczny”). Szyfrowanie asymetryczne jest podstawową technologią TLS (często nazywaną SSL).

Dlaczego szyfrowanie danych jest konieczne?

Prywatność: szyfrowanie zapewnia, że nikt nie może odczytać komunikacji lub danych w spoczynku, z wyjątkiem zamierzonego odbiorcy lub prawowitego właściciela danych., Uniemożliwia to atakującym, sieciom reklamowym, dostawcom usług internetowych, a w niektórych przypadkach rządom przechwytywanie i odczytywanie poufnych danych.

Bezpieczeństwo: Szyfrowanie pomaga zapobiegać naruszeniom danych, niezależnie od tego, czy dane są przesyłane, czy przechowywane. Jeśli urządzenie firmowe zostanie zgubione lub skradzione, a jego dysk twardy zostanie odpowiednio zaszyfrowany, dane na tym urządzeniu będą nadal bezpieczne. Podobnie zaszyfrowana komunikacja umożliwia stronom komunikującym wymianę poufnych danych bez wycieku danych.

Integralność danych: Szyfrowanie pomaga również zapobiegać złośliwym zachowaniem, takim jak ataki na ścieżce. Gdy dane są przesyłane przez Internet, szyfrowanie (wraz z innymi zabezpieczeniami integralności) zapewnia, że to, co odbiorca otrzymuje, nie zostało zmienione po drodze.

Uwierzytelnianie: szyfrowanie klucza publicznego, między innymi, może być wykorzystane do ustalenia, że właściciel witryny jest właścicielem klucza prywatnego wymienionego w certyfikacie TLS witryny. Pozwala to użytkownikom Witryny mieć pewność, że są połączeni z rzeczywistą witryną (zobacz, co to jest szyfrowanie klucza publicznego? aby dowiedzieć się więcej).,

Przepisy: z tych wszystkich powodów wiele przepisów branżowych i rządowych wymaga od firm, które przetwarzają dane użytkowników, aby te dane były szyfrowane. Przykłady norm regulacyjnych i zgodności, które wymagają szyfrowania, obejmują HIPAA, PCI-DSS i RODO.

Czym jest algorytm szyfrowania?

Algorytm szyfrowania jest metodą wykorzystywaną do przekształcania danych w tekst szyfrowy. Algorytm użyje klucza szyfrowania w celu zmiany danych w przewidywalny sposób, tak że nawet jeśli zaszyfrowane dane będą wyglądać losowo, mogą być z powrotem zamienione na zwykły tekst za pomocą klucza deszyfrującego.

Jakie są popularne algorytmy szyfrowania?

Powszechnie stosowane algorytmy szyfrowania symetrycznego obejmują kilka kluczowych metod, które są powszechnie używane ze względu na ich skuteczność i bezpieczeństwo.
Niektóre z najważniejszych:

1. **AES (Advanced Encryption Standard)**:

- **Opis**: AES jest najczęściej używanym algorytmem szyfrowania symetrycznego to szyfr blokowy. Jest standardem FIPS-197 amerykańskiego Narodowego Instytutu Standardów i Technologii (NIST) od 2001 roku.

- **Wielkość bloku wejściowego**: 128 bitów
- **Długość klucza:** Możliwe są trzy długości klucza: 128, 192 i 256 bitów.
- **Liczba rund:** Zależna od długości klucza: 10 rund dla 128-bitowego, 12 rund dla 192-bitowego i 14 rund dla 256-bitowego klucza.
- **Zastosowanie**: Bezpieczeństwo danych w wielu aplikacjach, od ochrony danych **rządowych** po szyfrowanie komunikacji w Internecie.

AES jest szeroko stosowany w celu ochrony danych przed nieuprawnionym dostępem oraz do szyfrowania komunikacji w Internecie. Jego zastosowania obejmują zarówno bezpieczeństwo danych rządowych, jak i komercyjnych aplikacji. Jest to również pierwszy publicznie dostępny szyfr, który został zatwierdzony i wykorzystywany przez NSA do ochrony ściśle tajnych informacji.

2. **DES (Data Encryption Standard)**:

- **Opis**: DES był standardem szyfrowania od lat 70. XX wieku aż do wprowadzenia AES. Algorytm DES działał na blokach o długości 64 bitów.
- **Klucze**: 56 bitów, co jest obecnie uważane za niewystarczające ze względu na podatność na ataki brute-force.
- **Zastosowanie**: Choć jest obecnie rzadziej używany, DES wciąż można spotkać w starszych systemach i aplikacjach, które nie przeszły na bardziej zaawansowane metody szyfrowania.

Ze względu na swoją krótką długość klucza DES jest podatny na ataki, a jego stosowanie nie jest już zalecane w nowych systemach. Współczesne standardy, takie jak AES, oferują znacznie lepsze zabezpieczenia.

3. **3DES (Triple DES)**:

- **Opis**: 3DES jest rozwinięciem DES, które trzykrotnie szyfruje dane, co znacząco zwiększa bezpieczeństwo w porównaniu do samego DES.
- **Klucze**: Efektywnie 168 bitów (3x56 bitów).
- **Zastosowanie**: Bezpieczne transmisje danych, bankowość i inne zastosowania wymagające wyższego poziomu bezpieczeństwa. Przykłady zastosowań to bezpieczne transmisje danych, bankowość oraz inne obszary, gdzie ochrona informacji jest kluczowa.

3DES jest bardziej odporny na ataki niż oryginalny DES, ale ze względu na swoją długość klucza i wydajność, coraz częściej zastępowany jest przez bardziej zaawansowane algorytmy, takie jak AES.

4. **Blowfish**:

- **Opis**: Blowfish to szybki algorytm szyfrowania symetrycznego zaprojektowany przez Bruce'a Schneiera. Jest znany ze swojej elastyczności pod względem długości klucza i wydajności. Blokowy szyfr o długości bloku 64 bitów.
- **Klucze**: Od 32 do 448 bitów.
- **Zastosowanie**: Algorytm Blowfish był popularny w latach 90., szczególnie oprogramowanie, takie jak systemy operacyjne oraz różne aplikacje, które potrzebują szybkiego i elastycznego szyfrowania.

Obecnie jest jednak coraz rzadziej stosowany, istnieją bardziej bezpieczne i wydajne alternatywy jego miejsce często zajmuje bardziej zaawansowany AES.

5. **Twofish**:

- **Opis**: Twofish to symetryczny szyfr blokowy, rozwinięcie Blowfish, również zaprojektowane przez Bruce'a Schneiera. Jest jednym z finalistów konkursu na AES. Nadal można go używać jako bezpiecznego narzędzia do ochrony prywatnych informacji.
- **Klucze**: działa z kluczami o długości 128, 192 lub 256 bitów.
- **Zastosowanie**: Szyfrowanie danych w aplikacjach i systemach, które wymagają wysokiego poziomu bezpieczeństwa.

Wykorzystuje pre-obliczone S-boksy zależne od klucza oraz stosunkowo złożony harmonogram klucza. Mimo że AES ostatecznie go zastąpił, nadal pozostaje interesującym algorytmem.

6. **RC4**:

- **Opis**: RC4 to algorytm szyfrowania strumieniowego, znany z prostoty i szybkości. Jednak ze względu na znane słabości nie jest już uważany za bezpieczny.
- **Klucze**: Do 2048 bitów (w praktyce zazwyczaj 40 do 128 bitów).
- **Zastosowanie**: Był szeroko stosowany w protokołach takich jak WEP (Wireless Equivalent Privacy) i TLS (Transport Layer Security).

RC4 nie jest już uważany za bezpieczny i nie jest rekomendowany do nowych implementacji.

7. **ChaCha20**:

- **Opis**: ChaCha20 to nowoczesny algorytm szyfrowania strumieniowego, zaprojektowany przez Daniela Bernsteina. Jest znany ze swojej wysokiej wydajności i bezpieczeństwa. jest alternatywą dla algorytmu RC4 i oferuje wyższą wydajność oraz bezpieczeństwo. Jest to szyfr strumieniowy, co oznacza, że działa na pojedynczych bajtach danych w przeciwieństwie do szyfrów blokowych, które operują na blokach danych.
- **Klucze**: 256 bitów.
- **Zastosowanie**: Szyfrowanie komunikacji internetowej, takich jak w protokołach TLS (np. w HTTPS) oraz w aplikacjach mobilnych. Jego wydajność i bezpieczeństwo sprawiają, że jest popularnym wyborem w wielu nowoczesnych systemach.

Uważany za bezpieczny i rekomendowany jako alternatywa dla starszych algorytmów, takich jak RC4.

Te algorytmy są powszechnie stosowane w różnych zastosowaniach, od zabezpieczania komunikacji internetowej, przez ochronę danych przechowywanych na urządzeniach, po zabezpieczanie transakcji finansowych. Każdy z nich ma swoje specyficzne właściwości i zastosowania, co czyni je odpowiednimi do różnych scenariuszy bezpieczeństwa.

Powszechnie stosowane algorytmy szyfrowania asymetrycznego obejmują kilka kluczowych metod, które są szeroko używane ze względu na ich unikalne właściwości i zastosowania w kryptografii. Najważniejsze z nich:

1. **RSA (Rivest-Shamir-Adleman)**:

- **Opis**: RSA jest jednym z najstarszych i najczęściej stosowanych algorytmów szyfrowania asymetrycznego z kluczem publicznym. Opiera się na trudności faktoryzacji dużych liczb pierwszych. Został zaprojektowany w 1977 roku przez Rona Rivesta, Adiego Shamira oraz Leonarda Adlemana.
- **Klucze**: Zazwyczaj od 1024 do 4096 bitów.
- **Generowanie kluczy:** Aby wygenerować parę kluczy (prywatny i publiczny), należy:
    1. Wybrać losowo dwie duże liczby pierwsze, p i q.
    2. Obliczyć wartość n = pq.
    3. Obliczyć φ(n) = (p-1)(q-1).
    4. Wybrać liczbę e (1 < e < φ(n)), która jest względnie pierwsza z φ(n).
    5. Znaleźć liczbę d, która jest odwrotnością modularną liczby e: d·e ≡ 1 (mod φ(n)).
    6. Klucz publiczny to para (n, e), a klucz prywatny to para (n, d).
- **Szyfrowanie i deszyfrowanie:** RSA dzieli wiadomość na bloki i stosuje następujące wzory:
- Szyfrowanie:

$$C = M^e \mod n$$

- Deszyfrowanie:

$$M = C^d \mod n$$

- **Zastosowanie**: Szyfrowanie danych, podpisy cyfrowe, bezpieczna wymiana kluczy, certyfikaty SSL/TLS.

RSA jest fundamentem wielu technologii bezpieczeństwa, a jego bezpieczeństwo jest nadal aktualne.

2. **ECC (Elliptic Curve Cryptography**) jest metodą kryptografii klucza publicznego opartą na strukturze algebraicznej krzywych eliptycznych nad skończonymi polami. W przeciwieństwie do kryptosystemów opartych na modularnej potęgowaniu w polach Galois, takich jak RSA czy ElGamal, ECC pozwala na stosowanie mniejszych kluczy, zachowując równoważne bezpieczeństwo:

- **Opis**: ECC wykorzystuje właściwości krzywych eliptycznych do tworzenia bezpiecznych i wydajnych systemów kryptograficznych. Oferuje podobny poziom bezpieczeństwa co RSA przy znacznie krótszych kluczach. Można go stosować w zakresie umawiania kluczy, podpisów cyfrowych, generatorów pseudolosowych i innych zadań. Pośrednio może być używany do szyfrowania, łącząc umawianie kluczy z symetrycznym schematem szyfrowania.
- **Klucze**: Zazwyczaj od 160 do 521 bitów. W porównaniu do innych metod, ECC oferuje podobny poziom bezpieczeństwa przy znacznie krótszych kluczach.

- **Zastosowanie**:
  - **Szyfrowanie danych**: ECC może być używane do bezpiecznego przesyłania poufnych informacji.
  - **Podpisy cyfrowe**: ECC umożliwia weryfikację autentyczności i integralności danych.
  - **Bezpieczna wymiana kluczy**: Protokoły takie jak Diffie-Hellman oparte na ECC pozwalają na bezpieczną wymianę kluczy między stronami.
  - **Certyfikaty SSL/TLS**: ECC jest stosowane w certyfikatach SSL/TLS, które zapewniają bezpieczne połączenia internetowe.
  - **Systemy mobilne i wbudowane**: Ze względu na swoją efektywność, ECC jest popularne w urządzeniach o ograniczonych zasobach.

3. **DSA (Digital Signature Algorithm)** to kryptosystem klucza publicznego i standard Federalnej Normy Przetwarzania Informacji (FIPS) do generowania podpisów cyfrowych. DSA opiera się na matematycznym pojęciu modularnej potęgi oraz problemie logarytmu dyskretnego.:

- **Opis**: DSA wykorzystuje klucze publiczne i prywatne do generowania i weryfikacji podpisów cyfrowych. Podpis cyfrowy zapewnia uwierzytelnienie, integralność i niemożliwość zaprzeczenia (sender nie może fałszywie twierdzić, że nie podpisał wiadomości). DSA jest wariantem schematów podpisów Schnorra i ElGamala.
- **Klucze**: Zazwyczaj od 1024 do 3072 bitów. W porównaniu do innych metod, DSA oferuje bezpieczeństwo przy stosunkowo krótszych kluczach.
- **Zastosowanie**:
  - **Podpisy cyfrowe**: DSA umożliwia generowanie podpisów cyfrowych, które potwierdzają autentyczność i integralność danych.
  - **Uwierzytelnianie**: DSA może być używane do weryfikacji tożsamości i autentyczności użytkowników lub systemów1.

  Standard FIPS 186-5 zakazuje generowania podpisów za pomocą DSA, ale pozwala na weryfikację podpisów wygenerowanych przed datą wdrożenia tego standardu. Współczesne schematy podpisów, takie jak EdDSA, zastępują DSA w nowych implementacjach.

4. **ElGamal**:

- **Opis**: ElGamal to algorytm oparty na logarytmach dyskretnych, wykorzystywany do szyfrowania i podpisów cyfrowych. ElGamal jest asymetrycznym algorytmem kryptograficznym, który opiera się na problemie obliczania logarytmów dyskretnych w skończonych ciałach. Algorytm ten został opisany przez Tahera Elgamala w 1985 roku. ElGamal jest wykorzystywany w oprogramowaniu takim jak GNU Privacy Guard (GPG), najnowsze wersje PGP oraz inne systemy kryptograficzne.
- **Klucze**: Zazwyczaj od 2048 bitów w górę. Klucz publiczny składa się z dwóch wartości: (g) (generator grupy cyklicznej) i (h). Klucz prywatny to liczba (x), która jest tajna i musi być zachowana w poufności.
- **Zastosowanie**:

- Szyfrowanie danych: Nadawca używa klucza publicznego odbiorcy do zaszyfrowania wiadomości, a odbiorca używa swojego klucza prywatnego do odszyfrowania.
- Podpisy cyfrowe: Algorytm ElGamala może być również używany do tworzenia bezpiecznych podpisów cyfrowych.
- Systemy wymiany kluczy: ElGamal jest stosowany w protokołach wymiany kluczy, takich jak Diffie-Hellman.

ElGamal jest nadal stosowany, ale zawsze warto sprawdzić najnowsze standardy i zalecenia dotyczące długości kluczy. Współczesne algorytmy kryptograficzne często wymagają kluczy o większej długości ze względu na rozwój obliczeniowej mocy atakujących

5. **Diffie-Hellman**:

- **Opis**: Diffie-Hellman to matematyczna metoda bezpiecznej wymiany kluczy kryptograficznych przez kanał publiczny, jest protokołem wymiany kluczy, który umożliwia dwóm stronom bezpieczne ustanowienie wspólnego tajnego klucza, który może być używany do szyfrowania symetrycznego.
- **Klucze**: Zazwyczaj od 2048 bitów w górę. Klucz publiczny składa się z dwóch wartości: (g) (generator grupy cyklicznej) i (h). Klucz prywatny to liczba (x), która jest tajna i musi być zachowana w poufności.
- **Zastosowanie**: Wymiana kluczy, zabezpieczanie komunikacji internetowej (np. w protokołach SSL/TLS). Zabezpieczanie komunikacji internetowej: Protokoły oparte na DH pozwalają na bezpieczne ustalenie kluczy sesji.

Badania z 2015 roku sugerują, że niektóre parametry DH używane w aplikacjach internetowych nie są wystarczająco silne, aby zapobiec atakom ze strony bardzo zasobnych przeciwników12

6. **Paillier**:

- **Opis**: Algorytm Pailliera, stworzony przez Pascala Pailliera w 1999 rokuto kryptosystem homomorficzny, który pozwala na operacje arytmetyczne na zaszyfrowanych danych bez ich odszyfrowywania. Paillier to probabilistyczny algorytm asymetryczny stosowany w kryptografii klucza publicznego. Problem obliczania klas reszt modulo (n) jest uważany za obliczeniowo trudny. Algorytm Pailliera opiera się na hipotezie decyzyjnej reszty złożonej (ang. decisional composite residuosity assumption).
- **Klucze**: Typowo od 1024 bitów w górę. Klucz publiczny składa się z dwóch wartości: (n) i (g), gdzie (n) jest iloczynem dwóch dużych liczb pierwszych (p) i (q). Klucz prywatny to liczba (λ(n)), która jest tajna i musi być zachowana w poufności.
- **Zastosowanie**: Specjalistyczne zastosowania, takie jak prywatne przetwarzanie danych i kryptografia homomorficzna. Homomorficzność: Paillier jest często wykorzystywany w systemach, które wymagają operacji na zaszyfrowanych danych, takich jak elektroniczne głosowanie.

Algorytm Pailliera jest często używany w kontekście kryptografii homomorficznej, która umożliwia przetwarzanie danych bez ich odszyfrowywania.

7. **RSA-OAEP (Optimal Asymmetric Encryption Padding)** to zaawansowany schemat dopełniania używany często w połączeniu z algorytmem RSA. Pozwala na zwiększenie bezpieczeństwa szyfrowania poprzez dodanie specjalnych mechanizmów paddingu.:

- **Opis**: RSA-OAEP jest często stosowany razem z algorytmem RSA, to udoskonalenie RSA, które wprowadza zabezpieczenia przeciwko niektórym typom ataków kryptograficznych poprzez użycie specjalnych schematów paddingu. Algorytm OAEP jest formą sieci Feistela, która używa dwóch tzw. "random oracle" (G i H) do przetwarzania tekstu jawnego przed zastosowaniem szyfrowania asymetrycznego.
- **Cele RSA-OAEP**:
  - Dodanie elementu losowości, co pozwala przekształcić deterministyczny schemat szyfrowania (np. tradycyjne RSA) w probabilistyczny.
  - Zapobieżenie częściowemu odszyfrowaniu szyfrogramów lub wyciekom informacji, poprzez uniemożliwienie odzyskania części tekstu jawnego bez umiejętności odwrócenia tzw. "trapdoor one-way permutation" (funkcji jednokierunkowej).
- **Klucze**: Zazwyczaj od 2048 do 4096 bitów.
- **Zastosowanie**: Szyfrowanie danych, bezpieczna wymiana kluczy, protokoły SSL/TLS.

Algorytmy szyfrowania asymetrycznego są kluczowe w wielu obszarach bezpieczeństwa informatycznego, zapewniając bezpieczne mechanizmy wymiany kluczy, podpisów cyfrowych i szyfrowania danych. Każdy z tych algorytmów ma swoje specyficzne właściwości, które czynią go odpowiednim do różnych zastosowań kryptograficznych.

Co to jest atak brute force w szyfrowaniu?

Atak brute force polega na tym, że atakujący, który nie zna klucza deszyfrującego, próbuje ustalić klucz, dokonując milionów lub miliardów domysłów. Ataki Brute force są znacznie szybsze w przypadku nowoczesnych komputerów, dlatego szyfrowanie musi być niezwykle silne i złożone. Większość nowoczesnych metod szyfrowania, w połączeniu z wysokiej jakości hasłami, są odporne na ataki brute force, chociaż mogą stać się podatne na takie ataki w przyszłości, jak komputery stają się coraz bardziej wydajne. Słabe hasła są nadal podatne na ataki brute force.

Co to jest szyfrowanie klucza publicznego?

Szyfrowanie klucza publicznego to rodzaj architektury szyfrowania zwanej kryptografią klucza publicznego, która wykorzystuje dwa klucze lub parę kluczy do szyfrowania i deszyfrowania danych. Jeden z dwóch kluczy jest kluczem publicznym, którego każdy może użyć do zaszyfrowania wiadomości dla właściciela tego klucza. Zaszyfrowana wiadomość jest wysyłana, a odbiorca używa swojego klucza prywatnego do jej odszyfrowania. Jest to podstawa szyfrowania klucza publicznego.

Ten rodzaj szyfrowania jest uważany za bardzo bezpieczny, ponieważ nie wymaga tajnego wspólnego klucza między nadawcą a odbiorcą. Inne technologie szyfrowania, które używają jednego klucza wspólnego do szyfrowania i deszyfrowania danych, polegają na tym, że obie strony decydują się na klucz z wyprzedzeniem, a inne strony nie dowiedzą się, co to jest klucz. Fakt, że musi być dzielony między obie strony, otwiera drzwi dla stron trzecich przechwytujących klucz. Ten rodzaj technologii

szyfrowania nazywa się szyfrowaniem symetrycznym, podczas gdy szyfrowanie kluczem publicznym jest znane jako szyfrowanie asymetryczne.

„Klucz” to po prostu mały fragment kodu tekstowego, który uruchamia powiązany algorytm do kodowania lub dekodowania tekstu. W szyfrowaniu klucza publicznego para kluczy jest generowana za pomocą programu szyfrującego, a para jest powiązana z nazwą lub adresem e-mail.
Klucz publiczny można następnie upublicznić, publikując go na serwerze kluczy, komputerze, na którym znajduje się baza kluczy publicznych. Alternatywnie klucz publiczny można udostępnić w sposób dyskryminujący, wysyłając go e-mailem do znajomych i współpracowników.
Osoby posiadające klucz publiczny mogą go używać do szyfrowania wiadomości do osoby lub adresu e-mail, z którym jest powiązany. Po otrzymaniu zaszyfrowanej wiadomości klucz prywatny osoby ją odszyfruje.

Szyfrowanie kluczem publicznym jest szczególnie przydatne do zachowania poufności wiadomości e-mail. Wszelkie wiadomości przechowywane na serwerach pocztowych, które mogą trwać przez lata, będą nieczytelne, a wiadomości przesyłane również będą nieczytelne. Ten stopień prywatności może wydawać się nadmierny, dopóki nie uświadomimy sobie otwartego charakteru Internetu.
Wysyłanie wiadomości e-mail w postaci niezaszyfrowanej jest podobne do upublicznienia dla każdego, kto czyta teraz lub w przyszłości.

Najbardziej znanym i cenionym programem szyfrującym klucz publiczny jest PGP (Pretty Good Privacy), który oferuje szyfrowanie na poziomie wojskowym. PGP ma wtyczki dla większości głównych klientów e-mail, dzięki czemu klienci współpracują z PGP, aby automatycznie szyfrować wiadomości wychodzące i odszyfrować wiadomości przychodzące. PGP utrzymuje „brelok” lub plik zebranych kluczy publicznych. Adres e-mail można powiązać z kluczem, dzięki czemu klient poczty e-mail automatycznie wybierze odpowiedni klucz publiczny z pierścienia klucza PGP, aby zaszyfrować wiadomość po wysłaniu. Będzie również automatycznie używał klucza prywatnego do odszyfrowywania poczty przychodzącej. Aby korzystać z szyfrowania klucza publicznego do wiadomości e-mail, zarówno nadawca, jak i odbiorca muszą mieć zainstalowane oprogramowanie szyfrujące.

Programy takie jak PGP mają również wbudowaną funkcję podpisu cyfrowego. Dzięki tej funkcji wysyłane wiadomości mogą być podpisane cyfrowo za pomocą jednego przycisku, dzięki czemu odbiorca wie, że wiadomość nie została zmieniona po drodze i jest autentyczna lub od określonego nadawcy. Szyfrowanie kluczem publicznym może być również wykorzystane do bezpiecznego przechowywania plików danych. W takim przypadku klucz publiczny służy do szyfrowania plików, a klucz prywatny odszyfrowuje je.

Szyfrowanie od końca do końca

Szyfrowanie od końca do końca (szyfrowanie end to end, E2EE) - system komunikacji, w którym wyłącznie osoby komunikujące się mogą odczytać wiadomości. W tym systemie, potencjalni podsłuchiwacze - w tym dostawcy Internetu bądź autorzy komunikatora - nie mogą uzyskać dostępu do kluczy szyfrujących potrzebnych do rozszyfrowania konwersacji.

W wielu systemach przesyłania wiadomości, w tym w poczcie elektronicznej i wielu komunikatorach internetowych, wiadomości przechodzą przez pośredników i są przechowywane przez stronę trzecią od której są pobierane przez odbiorcę. W większości komunikatorów, wiadomości szyfrowane są

wyłącznie w drodze od nadawcy do serwerów komunikatora oraz od serwerów komunikatora do adresata, a zatem są dostępne dla usługodawcy. Ma to wiele zalet, jak na przykład umożliwianie wyszukiwania tekstu w konwersacjach lub skanowania w poszukiwaniu nielegalnych lub nieodpowiednich treści, ale oznacza także, że wiadomości mogą być odczytane przez usługodawcę. Taki dostęp może być postrzegany jako ryzyko w wielu przypadkach, gdzie prywatność i poufność informacji jest bardzo ważna, na przykład w firmach, których reputacja zależy od umiejętności przechowywania danych użytkowników, negocjacji biznesowych oraz komunikacji na tyle ważnych, aby stały się celem hakowania lub inwigilacji oraz w organizacjach przechowujących dane zdrowotne bądź informacje o małoletnich.

Szyfrowanie od końca do końca ma na celu zapobieganie odczytywaniu lub modyfikacji danych przez osoby inne niż przez prawdziwego nadawcę i odbiorcę. Wiadomości są szyfrowane przez nadawcę, ale strona trzecia nie ma możliwości ich odszyfrowania i przechowuje je w postaci zaszyfrowanej. Odbiorcy pobierają zaszyfrowane dane i odszyfrowują je samodzielnie.

Ponieważ żadna osoba trzecia nie może odszyfrować przekazywanych lub przechowywanych danych, firmy stosujące takie szyfrowanie nie są w stanie przekazać władzom treści wiadomości swoich klientów.