Systemy Mobilne i Bezprzewodowe
laboratorium 12

Bezpieczeństwo i prywatność

Plan laboratorium

- Szyfrowanie,
- Uwierzytelnianie,
- Bezpieczeństwo systemów bezprzewodowych.

na podstawie :

- D. P. Agrawal, Q.-A. Zeng, *Introduction to Wireless and Mobile Systems*, 2e, Thomson, 2006
- Federal Information Processing Standards Publication, Fips Pub 46 - 3, Reaffirmed (1999) October 25, http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf
- Federal Information Processing Standards Publications (FIPS PUBS) 197, AES, (2001) November 26, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

Bezpieczeństwo i prywatność

- Transfer wiadomości w otwartym medium jakim jest przestrzeń powietrzna jest podatny na różne ataki
- Jednym z takich problemów jest „zagłuszanie” przez bardzo silną transmitującą antenę
- Problem można rozwiązać używając metody skakania po częstotliwościach w kolejnych odstępach czasu
- Używa się wielu technik szyfrowania, aby uniemożliwić nieautoryzowanym użytkownikom interpretację sygnałów

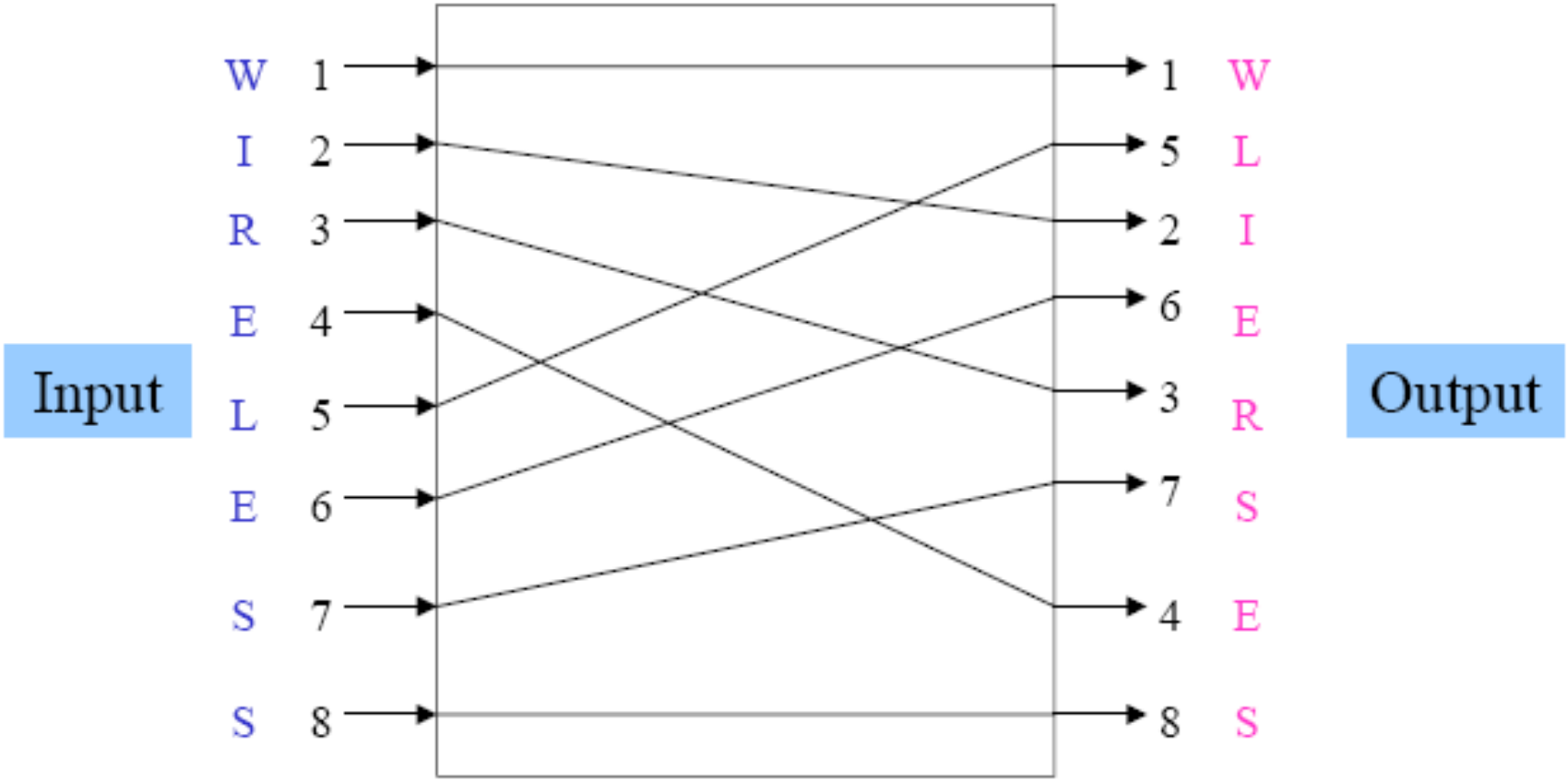
Dwie techniki szyfrowania

- Szyfrowanie z kluczem symetrycznym, np.:
  - DES (Data Encryption Standard), szyfr blokowy Feistel'a
  - AES (Advanced Encryption Standard), szyfr blokowy, sieć S-P
- Szyfrowanie z kluczem publicznym, np.:
  - RSA (od nazwisk twórców: Rivest, Shamir, Adleman), generator potęgowy

Szyfrowanie z kluczem symetrycznym

- Permutacja bitów przed ich transmisją w uprzednio zdefiniowany sposób – jeden z elementów szyfrowania
- Taka permutowana informacja może być odtworzona z użyciem operacji odwracającej
- Jednym z takich algorytmów jest DES (Data Encrytption Standard)

Funkcja prostej permutacji



Bity informacji przed transmisją oraz po ich otrzymaniu z użyciem DES

57	49	41	33	25	17	9	1
61	53	45	37	29	21	13	5
58	50	42	34	26	18	10	2
62	54	46	38	30	22	14	6
59	51	43	35	27	19	11	3
63	55	47	39	31	23	15	7
60	52	44	36	28	20	12	4
64	56	48	40	32	24	16	8

(a) Permutation before transmission

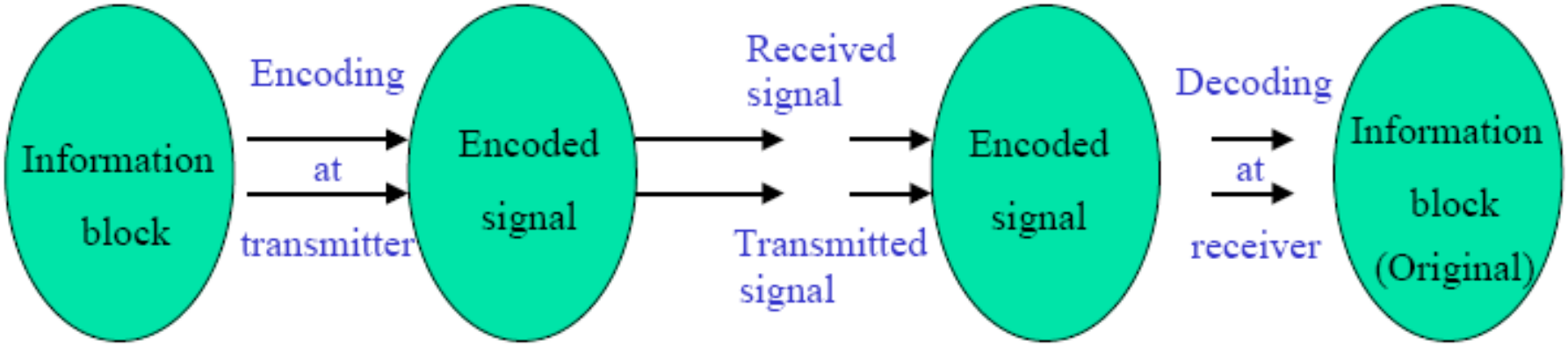
8	24	40	56	16	32	48	64
7	23	39	55	15	31	47	63
6	22	38	54	14	30	46	62
5	21	37	53	13	29	45	61
4	20	36	52	12	28	44	60
3	19	35	51	11	27	43	59
2	18	34	50	10	26	42	58
1	17	33	49	9	25	41	57

(b) Permutation after reception

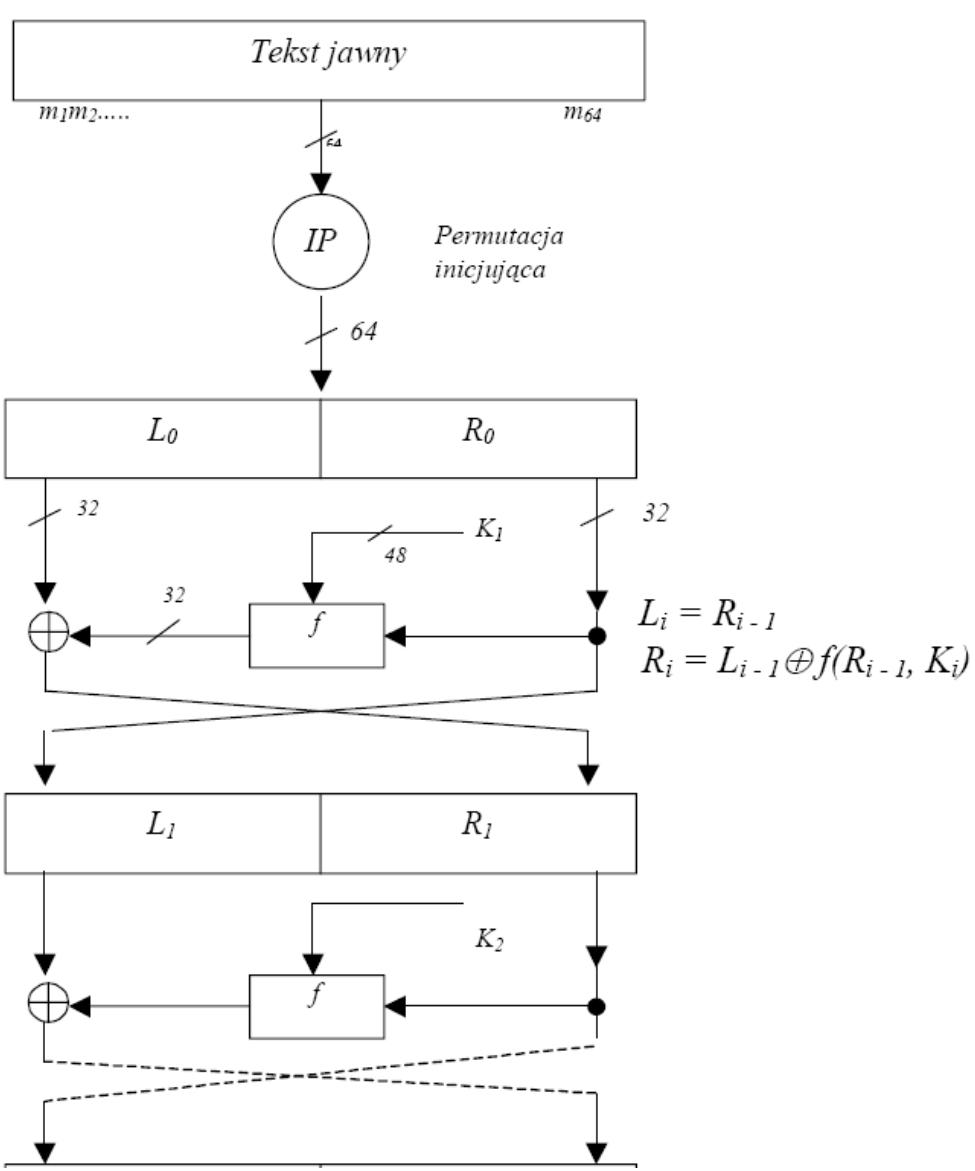
Szyfrowanie z kluczem symetrycznym

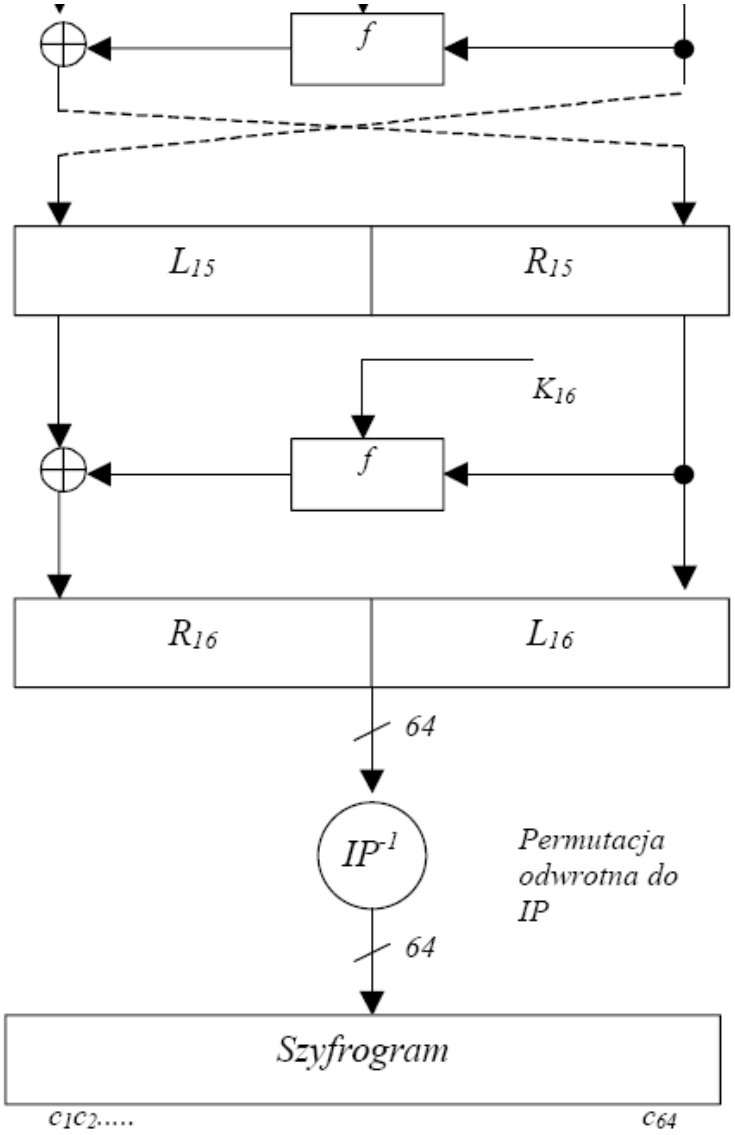
- Złożony schemat szyfrowania polega na transformacji bloków wejściowych w pewną zakodowaną formę
- Zakodowana informacja jest w sposób unikalny zamieniana na informację użyteczną
- Najprostsza transformacja zakłada logiczną lub arytmetyczną operację lub obie operacje

Proces kodowania i dekodowania

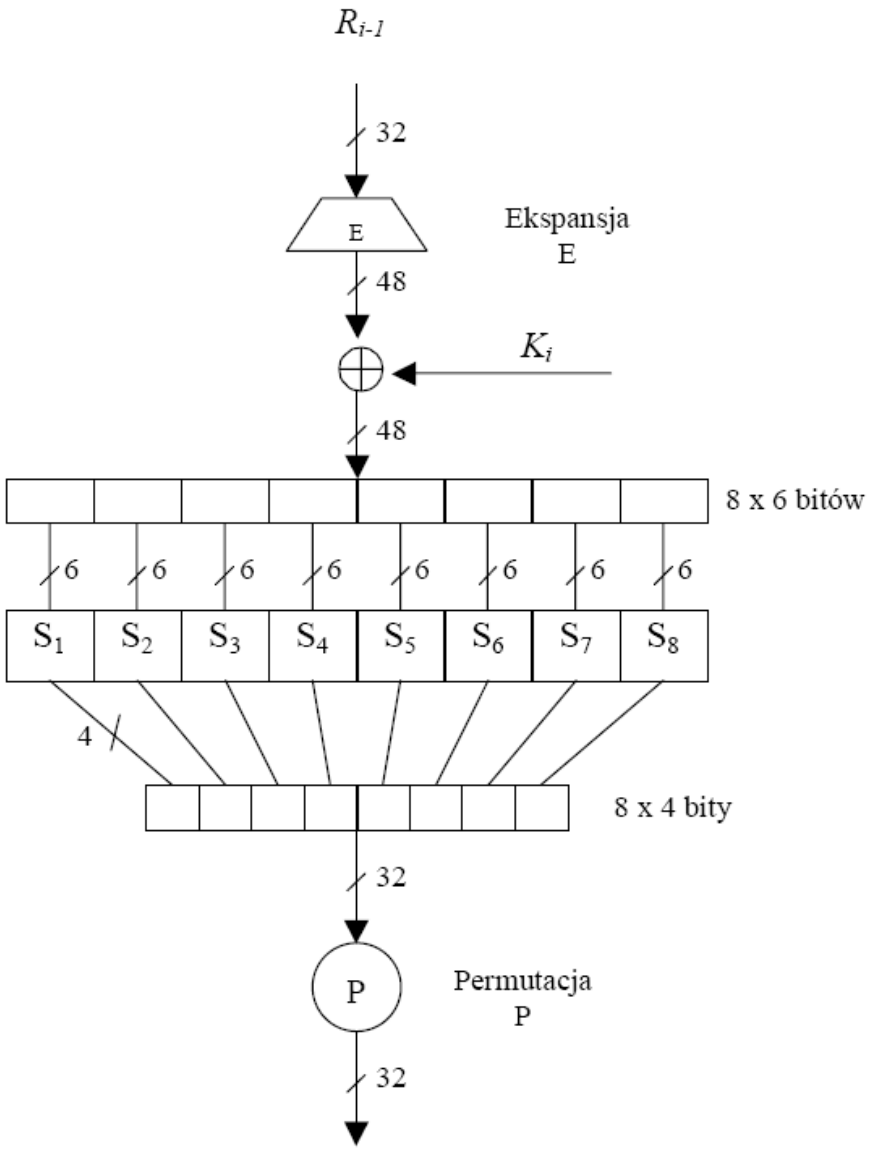


Permutacja i kodowanie informacji w DES





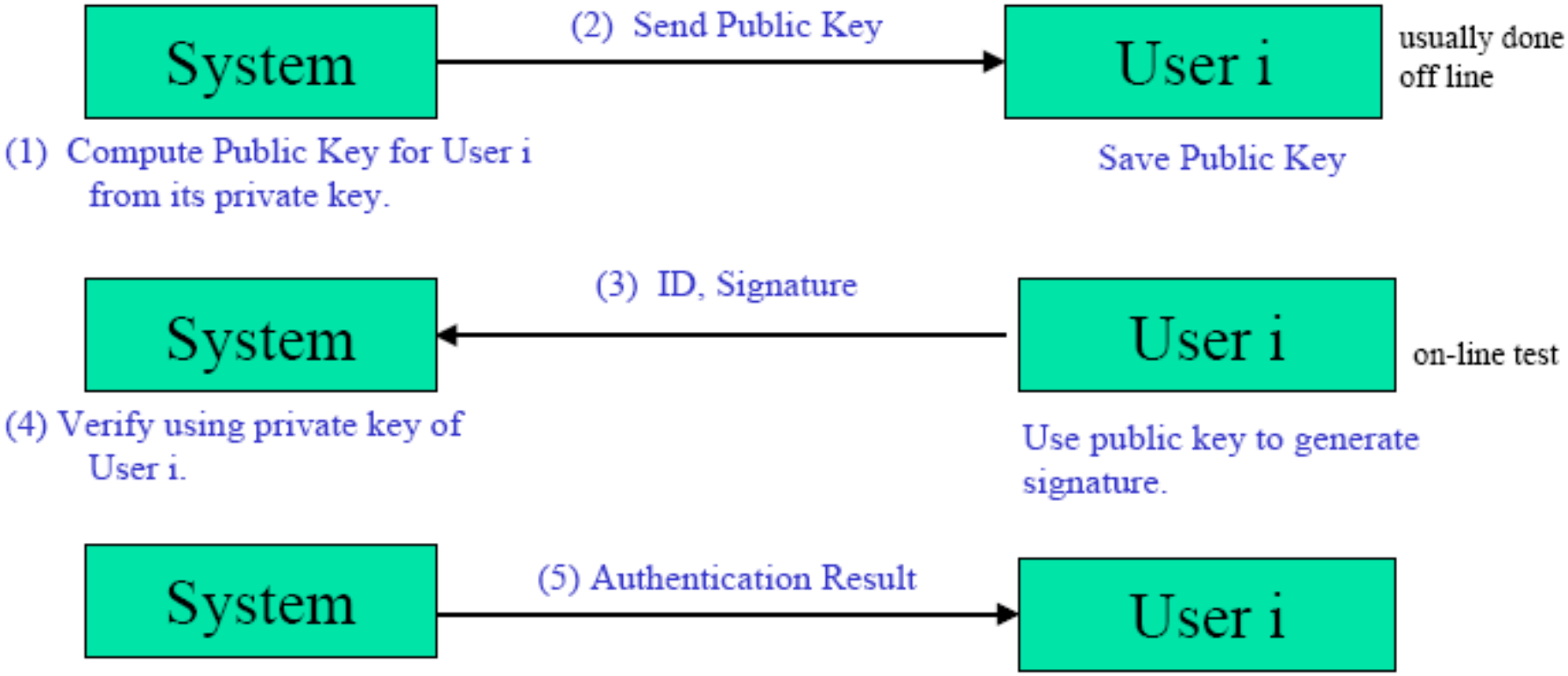
Transformacja f (stosująca S-Boxy)



Uwierzytelnianie

- Ma na celu upewnienie się, że użytkownik jest autentyczny
- Używa się funkcji haszującej działającej unikalnym identyfikatorze na związanej z użytkownikiem
- Inne podejście polega na użyciu dwóch związanych ze sobą kluczy (technika szyfrowania z kluczem publicznym)
- Jeden z nich znany jest tylko dla systemu generującego klucz (klucz prywatny), drugi klucz jest używany przy wysyłaniu do świata zewnętrznego (klucz publiczny)
- Algorytm RSA – najbardziej znany system z kluczem publicznym

Kroki uwierzytelnienia klucza publicznego/prywatnego



Uwierzytelnianie (Algorytm RSA)

- W algorytmie RSA 2 duże liczby pierwsze *(p, q)* są wybierane; *n=p*q*; wybiera się liczbę e w celu użycia (n,e) jako klucza publicznego i jest ona wysyłana do użytkownika.
- Użytkownik przechowuje ją i kiedykolwiek wiadomość *m<n* ma być wysłana, użytkownik oblicza

  i wysyła do systemu. Po otrzymaniu c system oblicza gdzie *d* jest obliczane na podstawie klucza prywatnego *(n,e)*

$$c^d|_{mod\ n}$$

$$c = m^e|_{mod\ n}$$

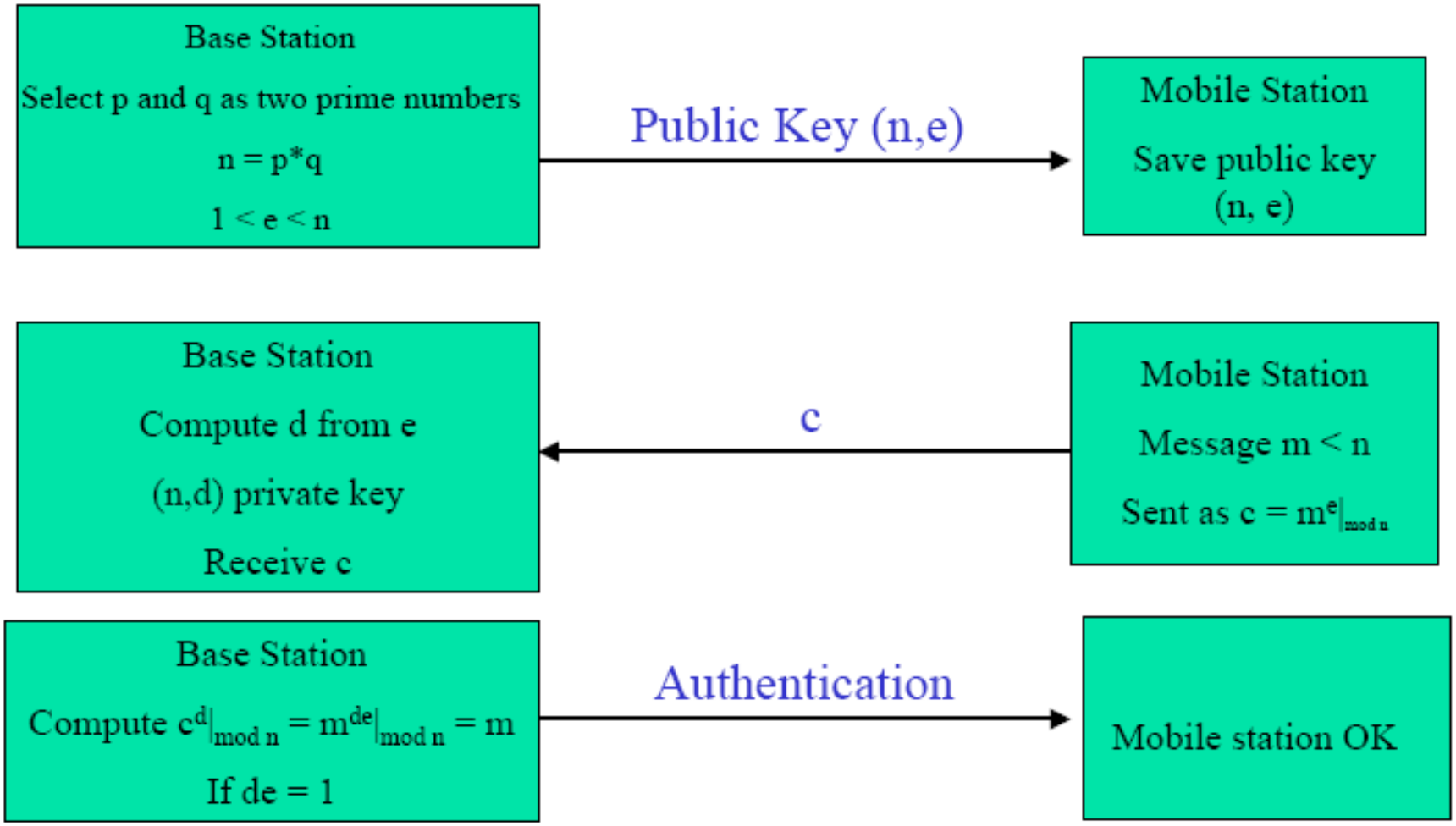
$$c^d|_{mod\ n} = (m^e|_{mod\ n})^d|_{mod\ n} = (m^e)^d|_{mod\ n}$$

$$= m^{ed}|_{mod\ n}$$

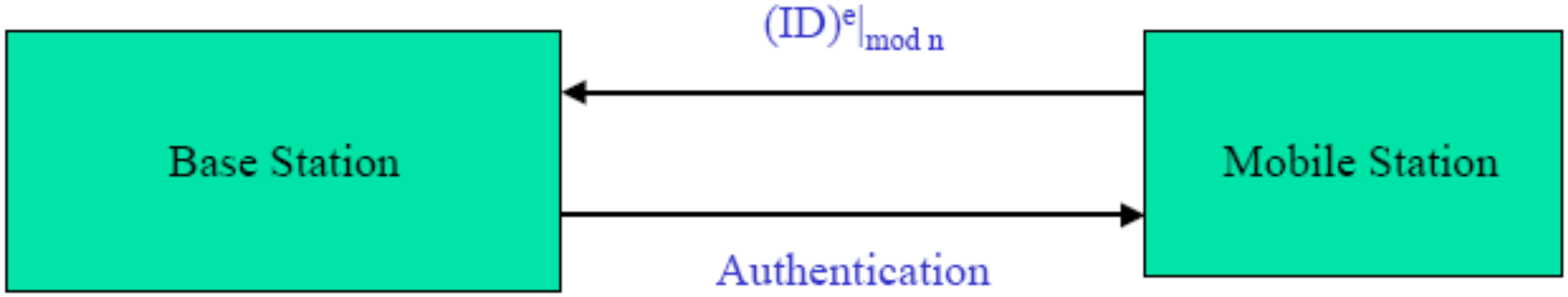
Uwierzytelnianie (Algorytm RSA) c.d.

- Aby miało to wartość równą *m*, *ed* musi być równe 1
- To oznacza, że *e* oraz *d* muszą być .. mod *n* (lub mod *p***q*)
- To może być spełnione jeżeli e jest liczbą pierwszą w stosunku do *(p-1)*(q-1)*
- Korzystając z tej zależności można uzyskać oryginalną wiadomość

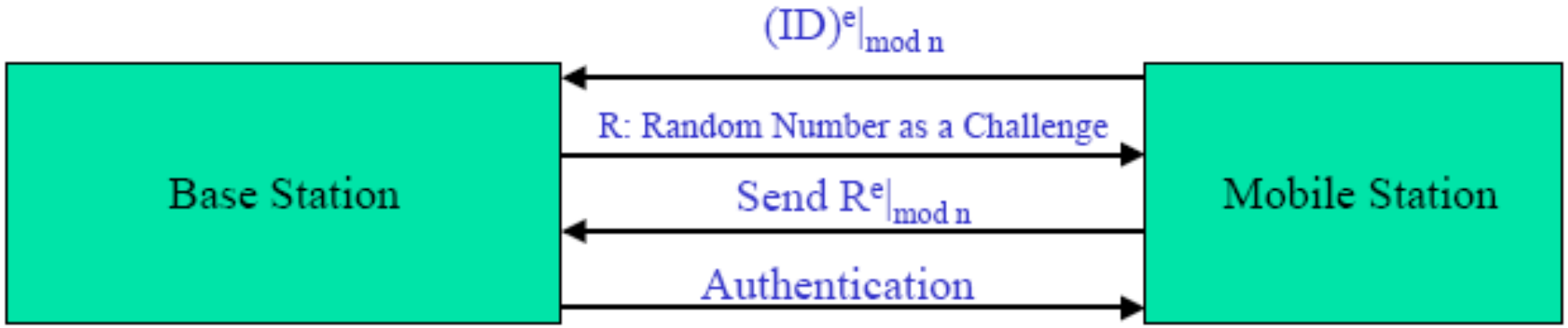
Uwierzytelnianie wiadomości przy użyciu klucza publicznego/prywatnego



Uwierzytelnianie MS-a przez BS



(a) Authentication based on ID



(b) Authentication using a challenge

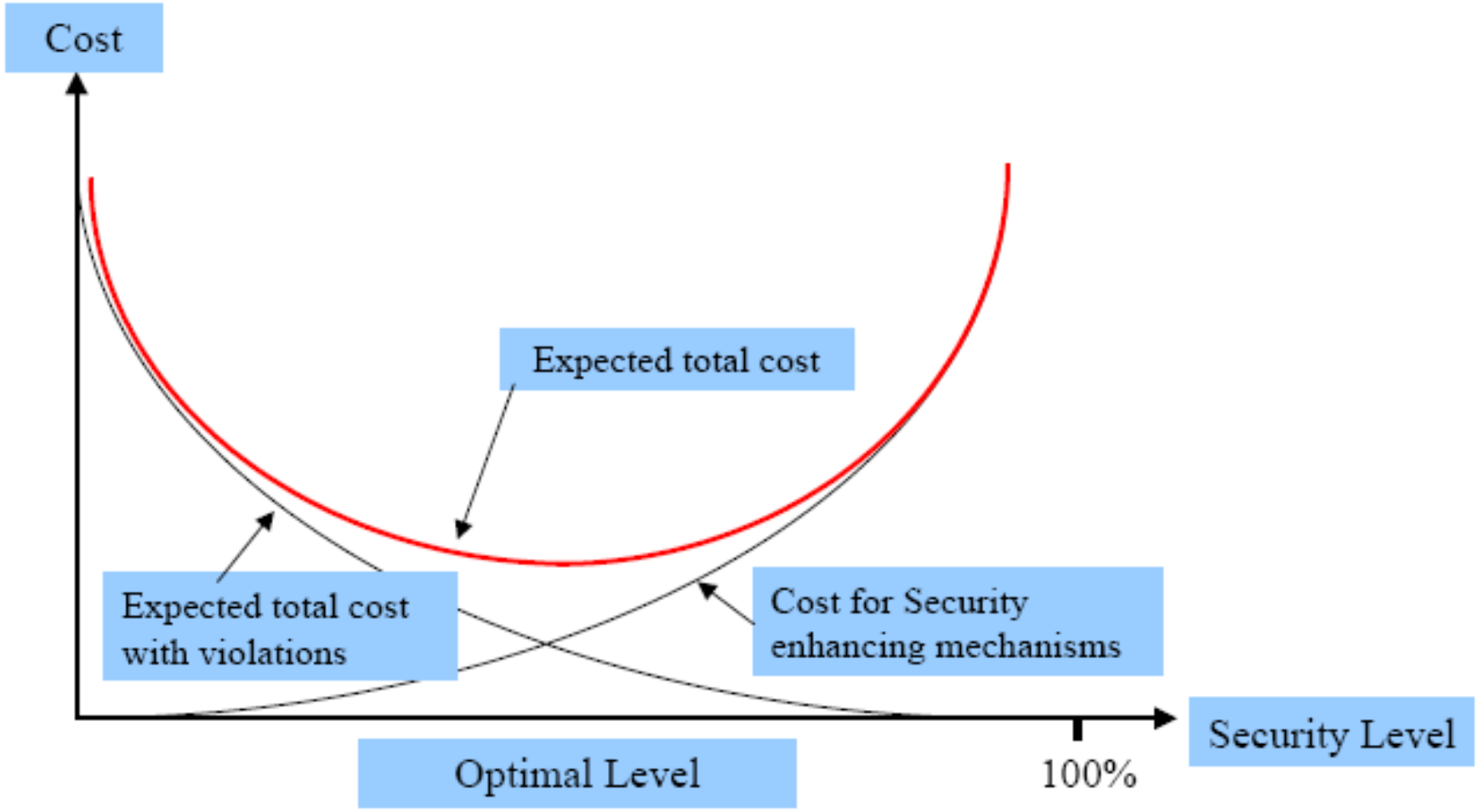
Bezpieczeństwo systemów bezprzewodowych

- Podstawowe usługi bezpieczeństwa:
  - Poufność - tylko autoryzowana strona może mieć dostęp do informacji systemu oraz transmitowanych danych
  - Niezaprzeczalność - nadawca i odbiorca nie mogą zaprzeczyć, że transmisja się odbyła
  - Uwierzytelnienie - nadawca informacji jest prawidłowo identyfikowany
  - Integralność - zawartość wiadomości może być modyfikowana tylko przez autoryzowanego użytkownika
  - Dostępność - zasoby są dostępne tylko dla autoryzowanych użytkowników

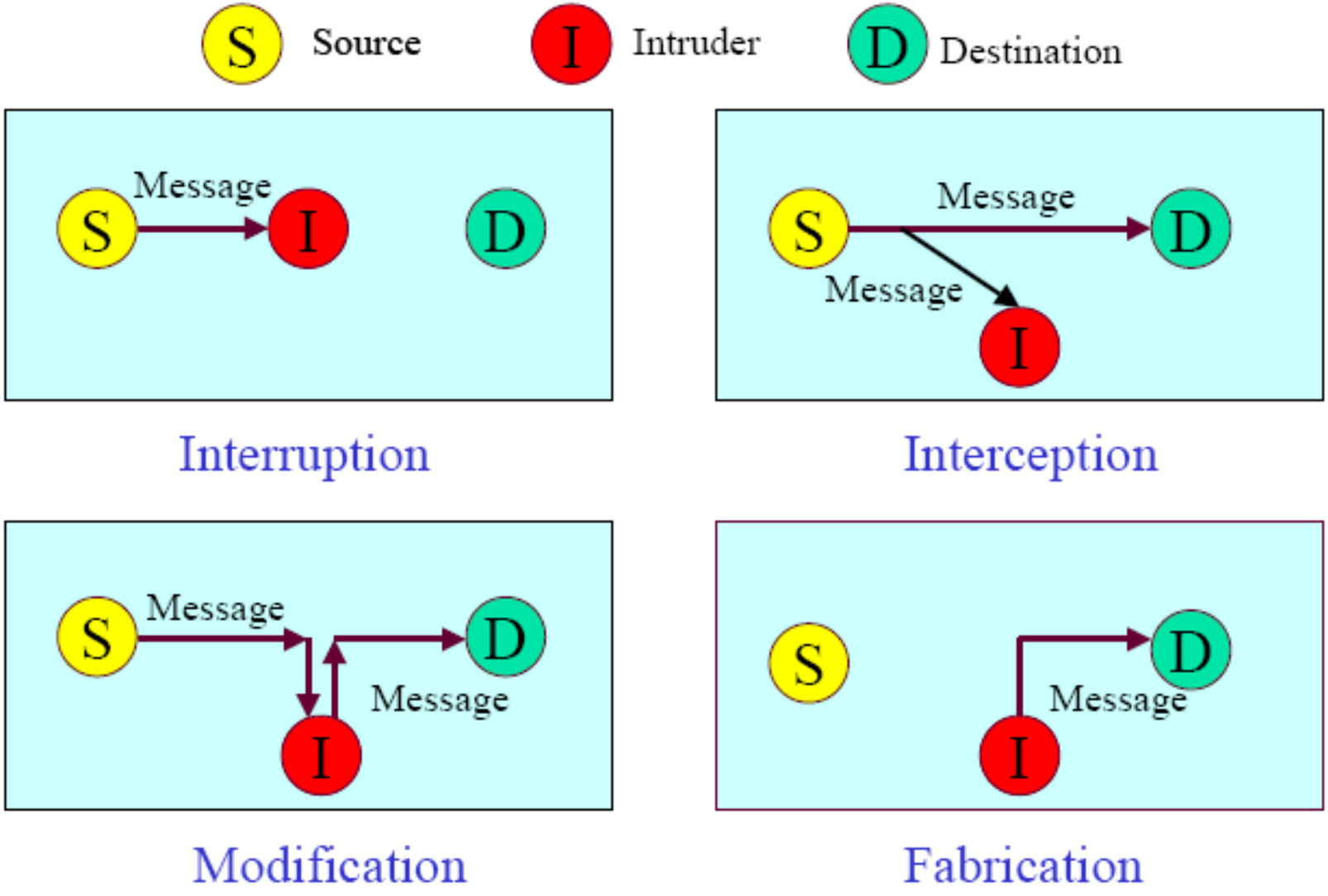
Bezpieczeństwo systemów bezprzewodowych

- Mechanizmy bezpieczeństwa:
  - Prewencja bezpieczeństwa - wymusza bezpieczeństwo w czasie funkcjonowania systemu
  - Detekcja bezpieczeństwa - odkrywa próby naruszenia bezpieczeństwa
  - Odtworzenie - odtwarzanie systemu do stanu przed naruszeniem bezpieczeństwa

Funkcja kosztu bezpiecznego systemu bezprzewodowego



Kategorie zagrożeń bezpieczeństwa (typy ataków)



Bezpieczeństwo bezprzewodowe

- Ataki aktywne - gdy ma miejsce modyfikacja danych lub fałszywa transmisja danych
  - Maskarada: dany podmiot pretenduje bycie innym podmiotem
  - Replay: przechwycenie informacji i jej retransmisja w celu wywołania nieautoryzowanego efektu
  - Modyfikacja wiadomości
  - Odmowa usługi (Denial of service – DoS)
- Pasywne ataki - celem intruza jest uzyskanie informacji (monitorowanie, podsłuchiwanie transmisji)